Safeguarding PII Training Course

Developed for:

Department of Defense

Defense Privacy and Civil Liberties Division

(DPCLD)

11/27/14

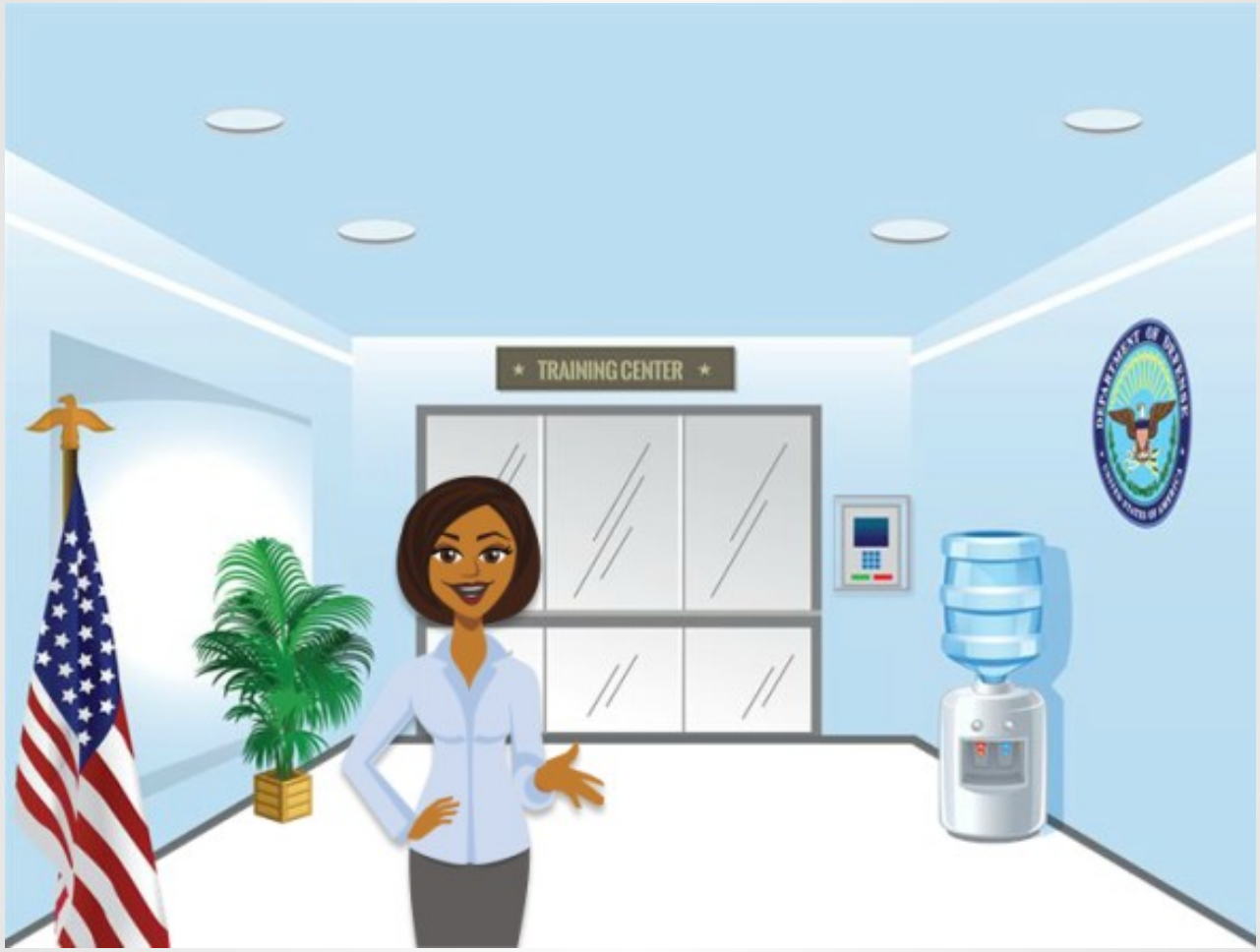
The following Microsoft PowerPoint presentation is designed as a supplemental outline to the interactive Safeguarding PII training course developed in Articulate Storyline.

Scene 1
Welcome & Introduction

1.1 Welcome

Narration: *Welcome to the Department of Defense Safeguarding Personally Identifiable Information (PII) Training. In this course, you will learn about the basic requirements of the DoD Privacy Program, and your critical role in protecting the PII maintained by the department.*

1.2 Training Greeting



Lena: *Hi, I'm Lena, your DoD Training Coordinator, thank you for attending our course. When you are ready, click on the security panel to join me in the training room for a brief orientation.*

1.3 Training Room

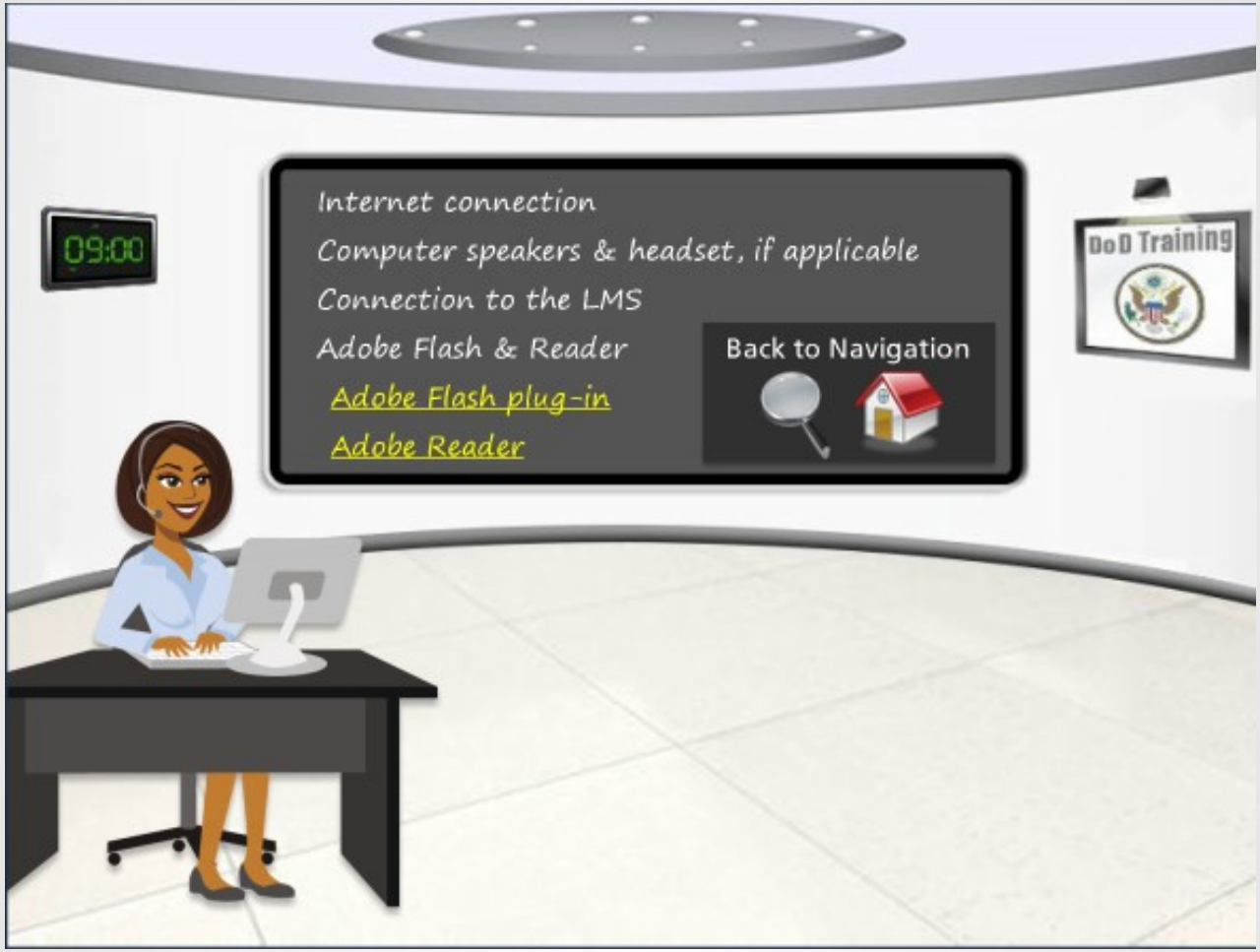
Lena: *To begin, let's review the navigation options and technical requirements for this course. To explore these features, click on the corresponding buttons on this screen.*

1.4 Course Navigation

Scene Description

The navigation options are displayed with markers to explore the menu links and navigation features of the course.

1.5 Technical Help



Scene Description
The technical requirements for the course are displayed including hyperlinks to download software applications.

1.6 Your Name

Lena: *To ensure you have a record of completing this course, please enter your name as you would like it to appear on your certificate. Select the Next button when you are ready.*

1.7 Course Mission

Lena: *Finally, it's time to learn more about the mission you're about to undertake.*

1.8 Course Design

Lena: *In this training exercise, you will embark on an important mission, requiring you to travel back in time to solve a case of identity theft. Along the way you will be presented with every day situations that require your intervention and problem-solving skills.*

1.9 Private C

Lena: *Today you will be taking on the role of Private C, a young service member who has been assigned to the newly formed US Temporal Command.*

1.9 General Relativity

Lena: *You will report directly to the head of TEMPCOM, General Relativity*

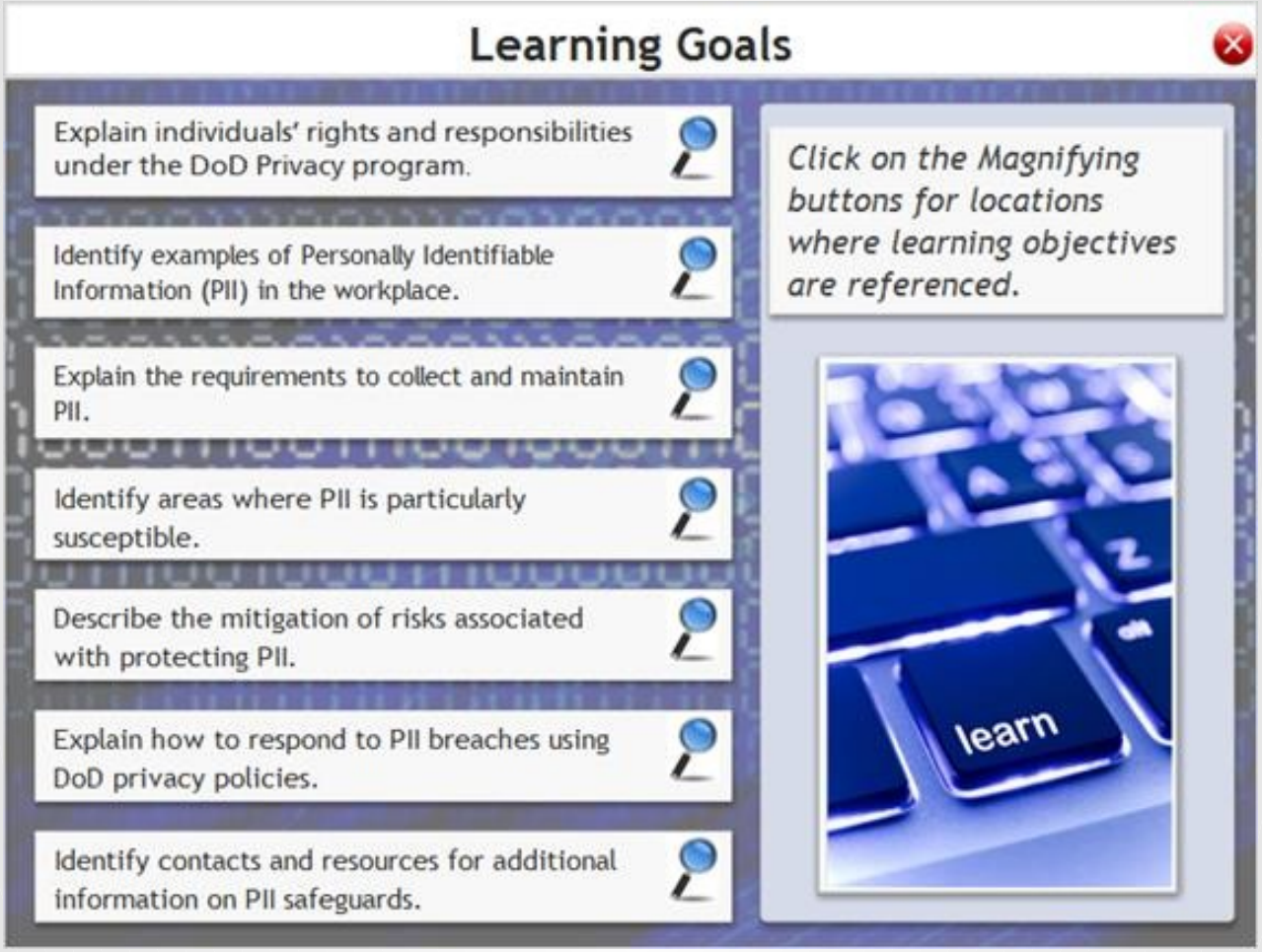
1.10 Captain Padlock

Lena: *Since today is your first day at TEMPCOM, General Relativity has asked Captain Padlock to help get you situated. She will be available throughout your mission to identify critical issues and provide expert advice.*

1.11 Start Mission

Captain Padlock: *Private C, Captain Padlock here... click on the Start button to begin your mission.*

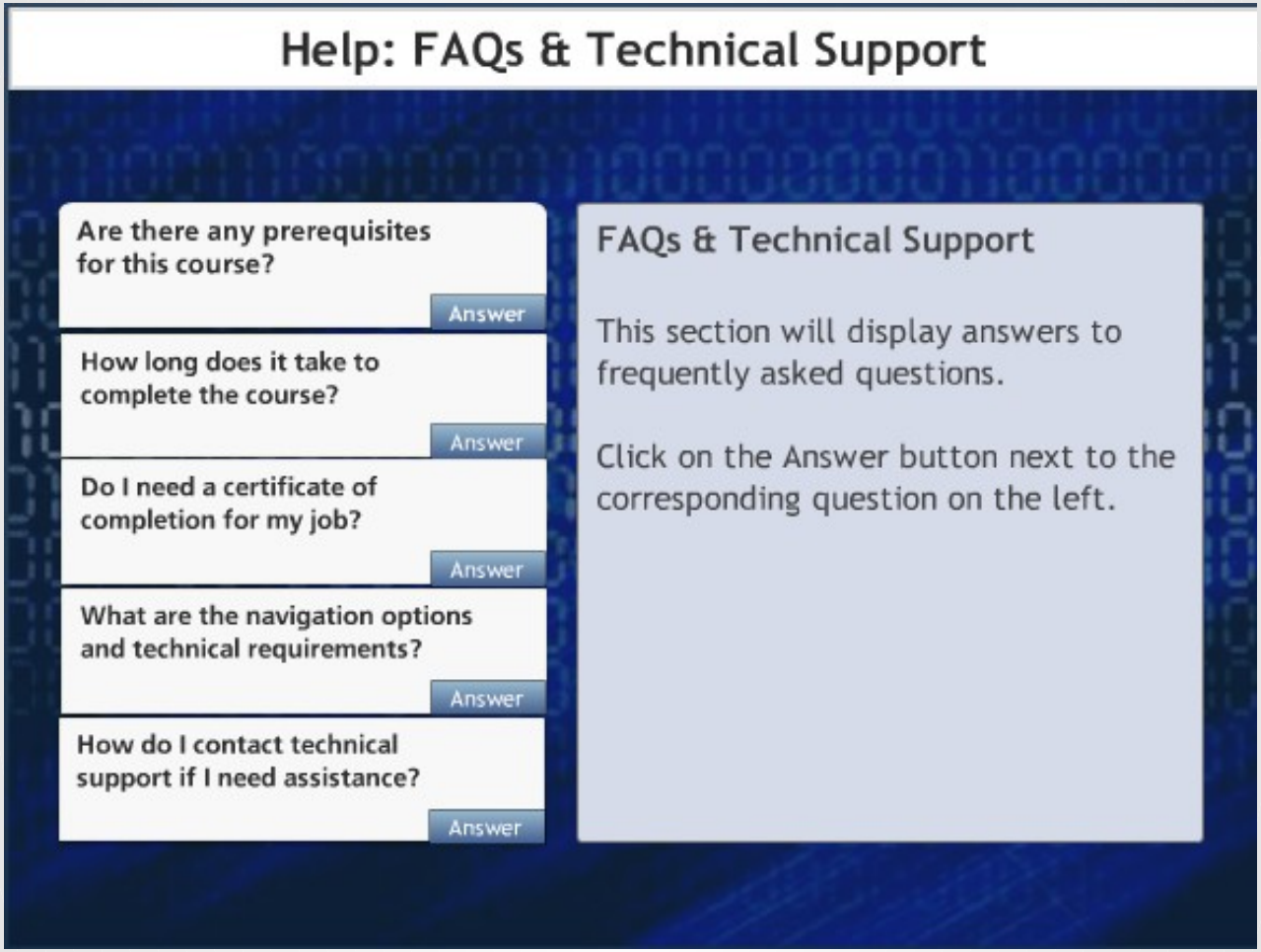
1.12 Learning Goals


Learning Goals
Explain individuals' rights and responsibilities under the DoD Privacy program.
Identify examples of Personally Identifiable Information (PII) in the workplace.
Explain the requirements to collect and maintain PII.
Identify areas where PII is particularly susceptible.
Describe the mitigation of risks associated with protecting PII.
Explain how to respond to PII breaches using DoD privacy policies.
Identify contacts and resources for additional information on PII safeguards.
Click on the Magnifying buttons for locations where learning objectives are referenced.
learn

Slide Description

List of course learning objectives with interactive buttons to navigate to related scenes.

1.13 Help


Help: FAQs & Technical Support
Are there any prerequisites for this course?
Answer
How long does it take to complete the course?
Answer
Do I need a certificate of completion for my job?
Answer
What are the navigation options and technical requirements?
Answer
How do I contact technical support if I need assistance?
Answer
FAQs & Technical Support
This section will display answers to frequently asked questions.
Click on the Answer button next to the corresponding question on the left.

Slide Description

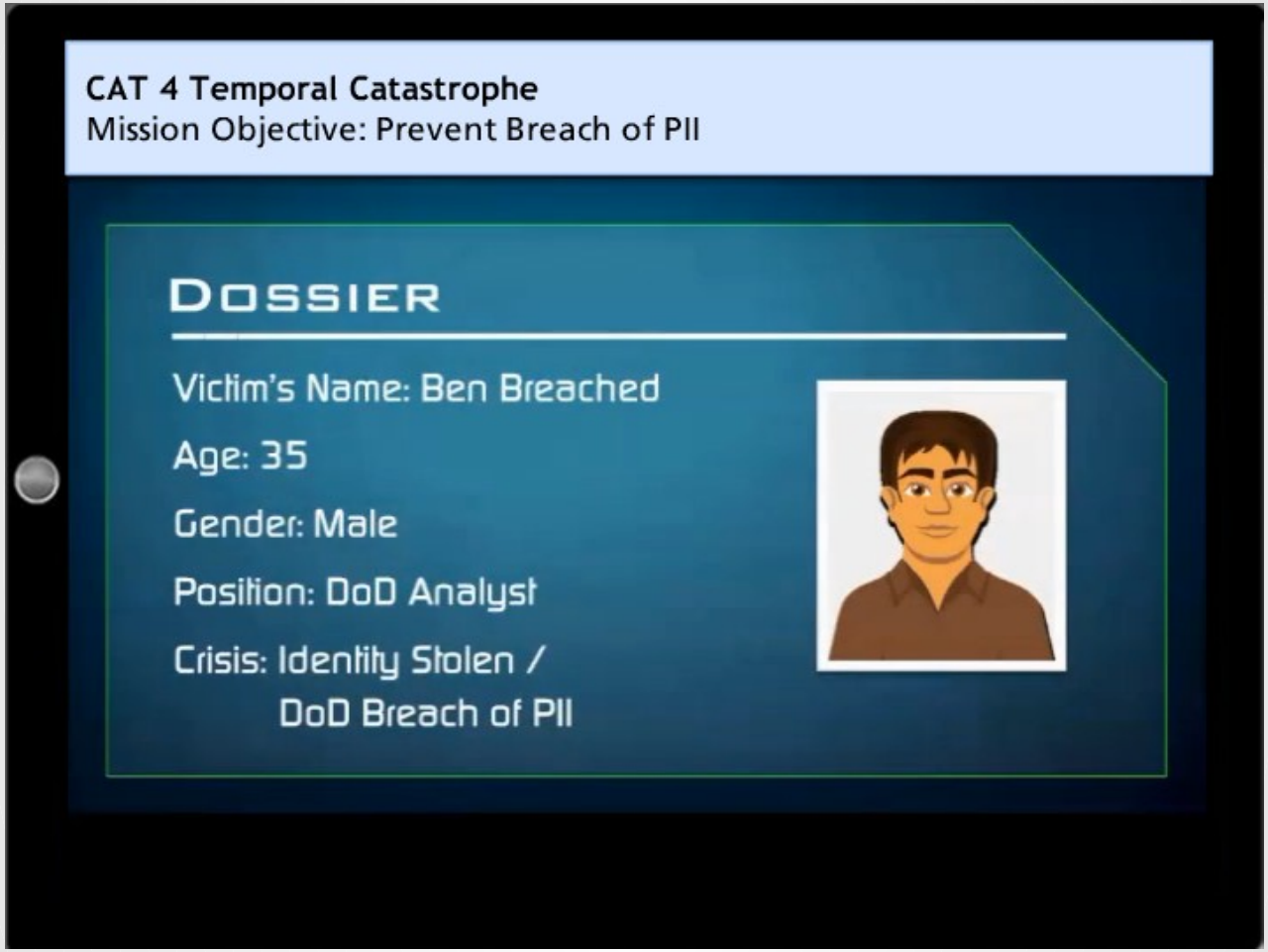
Information is provided on frequently asked questions and technical support.

Scene 2
U.S. Temporal Command

2.1 Mission Briefing

General Relativity: *Oh, Private C, I didn't see you come in. Please, take a seat. Welcome to US Temporal Command, we're happy to have you aboard. As you know, TEMPCOM specializes in the disruption and prevention of historic catastrophes through time travel insertion and extraction. I know it's your first day here, but there's no time for training wheels. We've just been alerted to a Category 4 Temporal Catastrophe, and we need you to stop it now! I've already uploaded the dossier to your tablet. Let's go over it now.*

2.2.1 Victim's Dossier

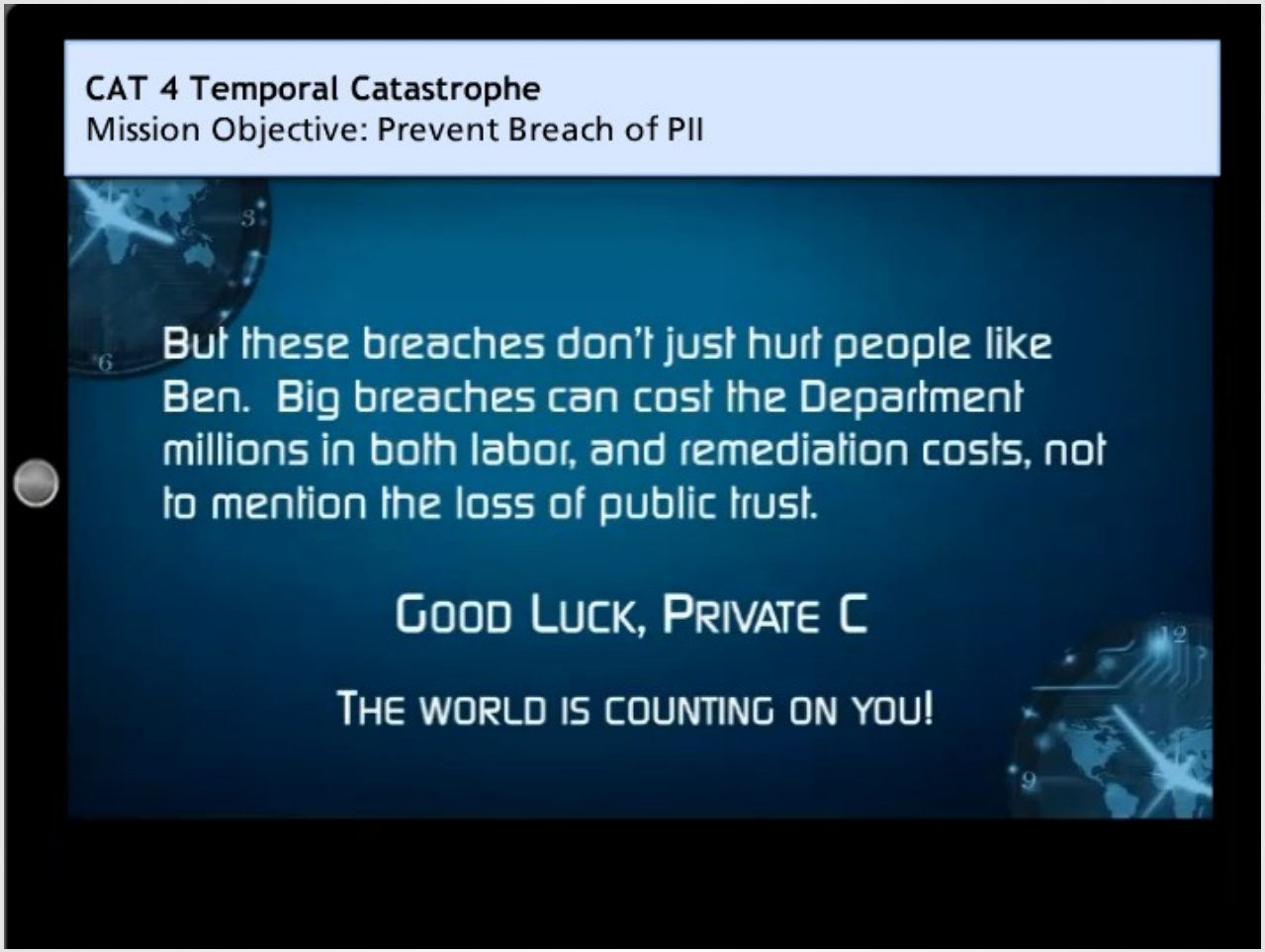


General Relativity: *This is Ben Breached. Several years ago he applied for a benefit with the Department. We collected his PII, to process the request, but somewhere along the line, that information found its way into the wrong hands. Today, Ben has been the target of numerous identity theft schemes.*

2.2.2 Victim's Dossier *(continued)*

General Relativity: *The results have been disastrous for him and his family. He had credit cards opened in his name and numerous bills rung up. Because of these fraudulent acts, he and his family have been hounded by debt collectors. He's spent thousands of dollars in legal costs and remediation efforts. His credit score has dropped, and his home has been placed in foreclosure. There are even criminal charges pending in another state for acts committed under his name and Social Security Number.*

2.2.3 Victim's Dossier *(continued)*


CAT 4 Temporal Catastrophe
Mission Objective: Prevent Breach of PII
But these breaches don't just hurt people like Ben. Big breaches can cost the Department millions in both labor, and remediation costs, not to mention the loss of public trust.
GOOD LUCK, PRIVATE C
THE WORLD IS COUNTING ON YOU!

General Relativity: *But these breaches don't just hurt people like Ben. Big breaches can cost the Department millions in both labor, and remediation costs, not to mention the loss of public trust.*

2.3 Report to Bootcamp

General Relativity: *We need you to go back in time now, find the source of this breach, and stop it before it ever happens. Don't worry, we're not sending you into the field alone. Captain Padlock will help guide you through this mission. Report to him immediately for Privacy Basic Training, so he can bring you up to speed on the Department's Privacy policies and practices.*

Scene 3
Privacy Training Bootcamp

3.1 Welcome to Privacy Training Bootcamp

Captain Padlock: *Private C, I'm glad you're here. Before we send you back in time, we need to get you comfortable with the basics of privacy. So let's get started.*

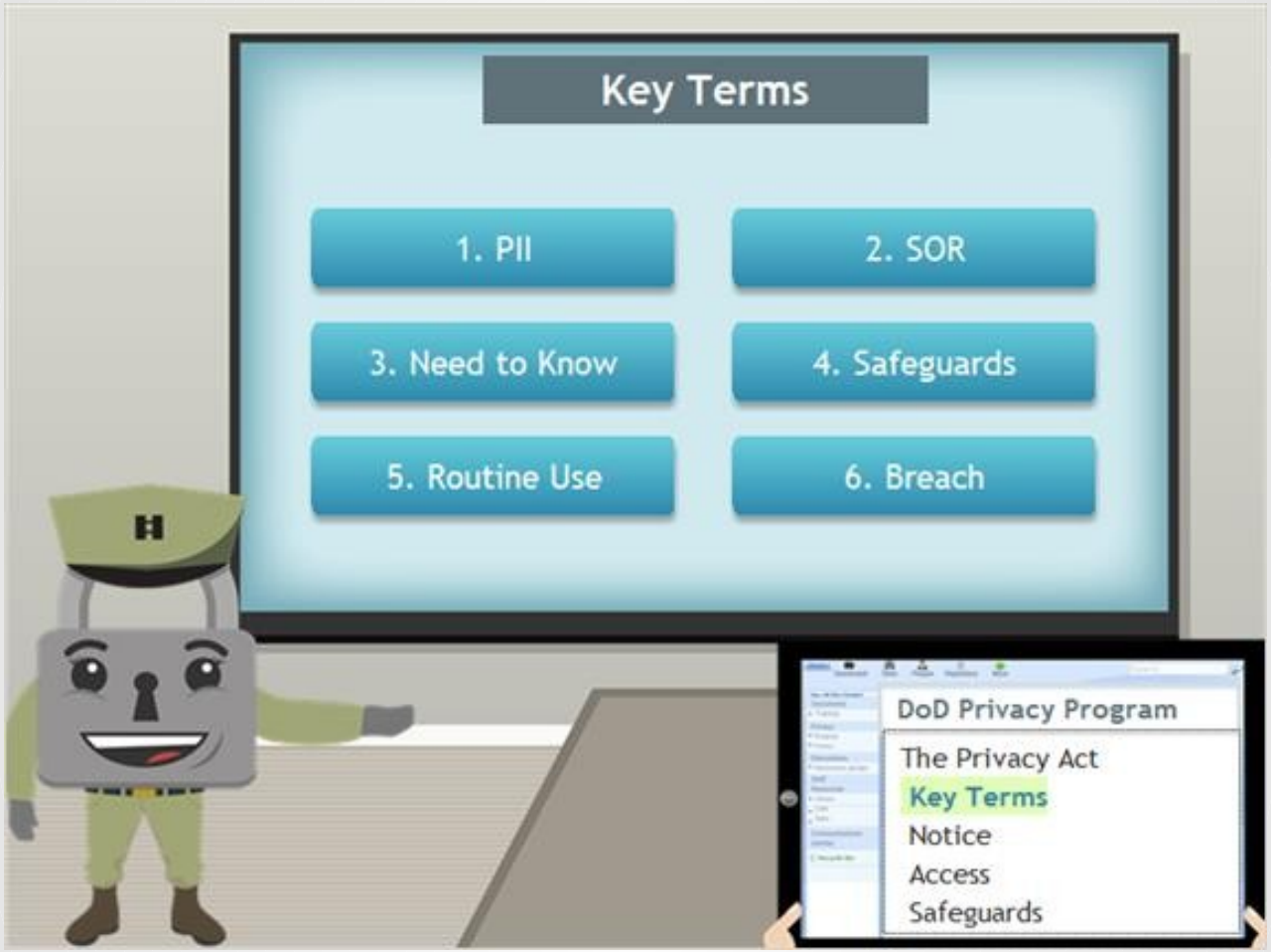
3.2 The Privacy Act

Captain Padlock: *Like all federal agencies, the DoD privacy program was established to comply with the Privacy Act of 1974. The Privacy Act was enacted in response to growing public concern over the government's collection, storage, and use of personal information. Incidents such as Watergate demonstrated the kind of power information and databases could have. Legislation was passed to make sure the public knew what the government intended to do with their information.*

3.3 Agency Requirements

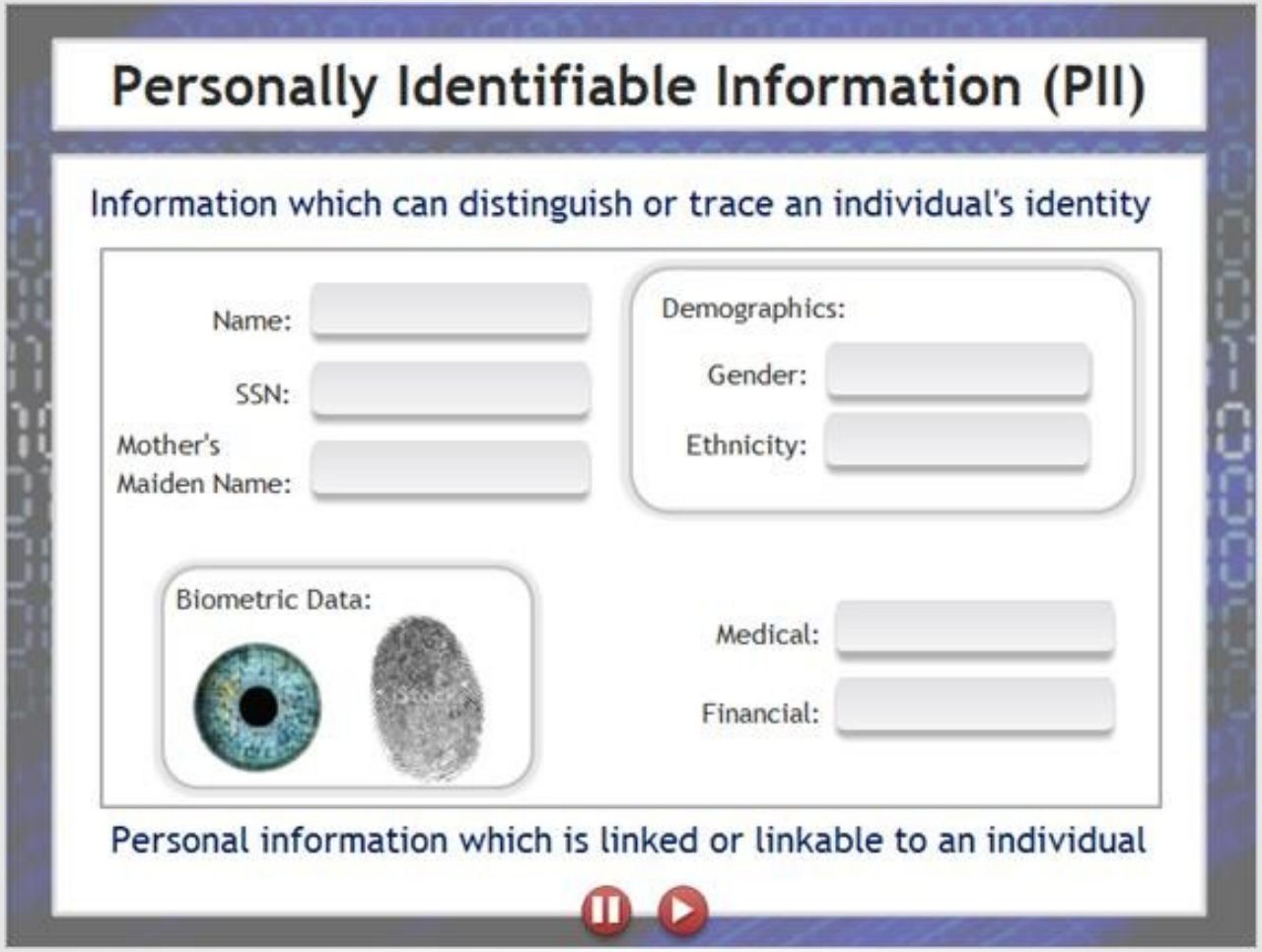
Captain Padlock: *To that end, the Privacy Act protects individuals by requiring Federal agencies, including DoD, to:*
1. Inform the public about the nature of all information collections.
2. Give an individual access to any records being held on them, including the right to ask that their records be corrected if there are errors or omissions.
3. Protect the information from unauthorized disclosures, breaches, or uses.

3.4 Key Terms



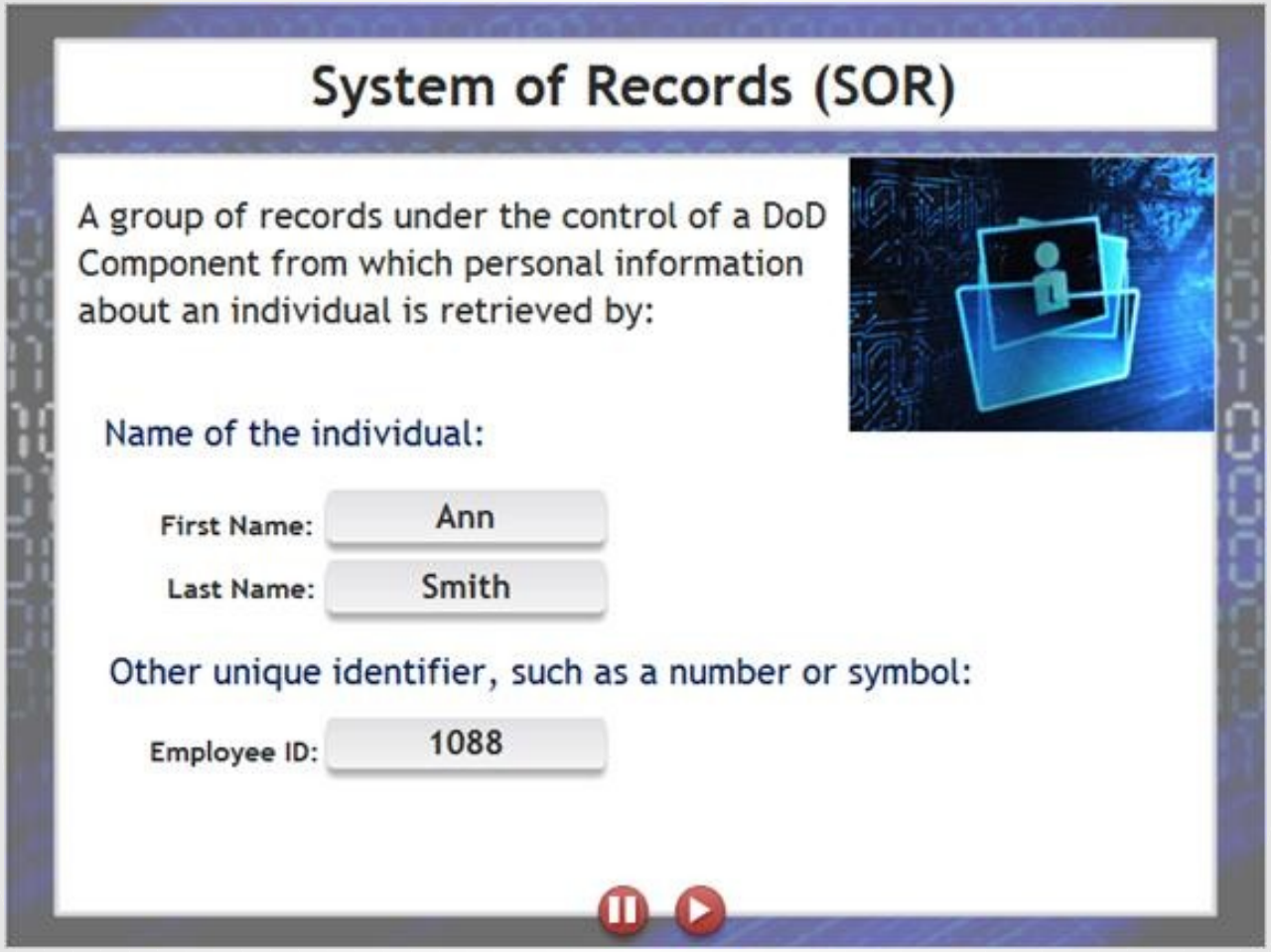
Captain Padlock: *Let's start with a few quick terms you'll need to be familiar with for this mission:*

3.4.1 PII



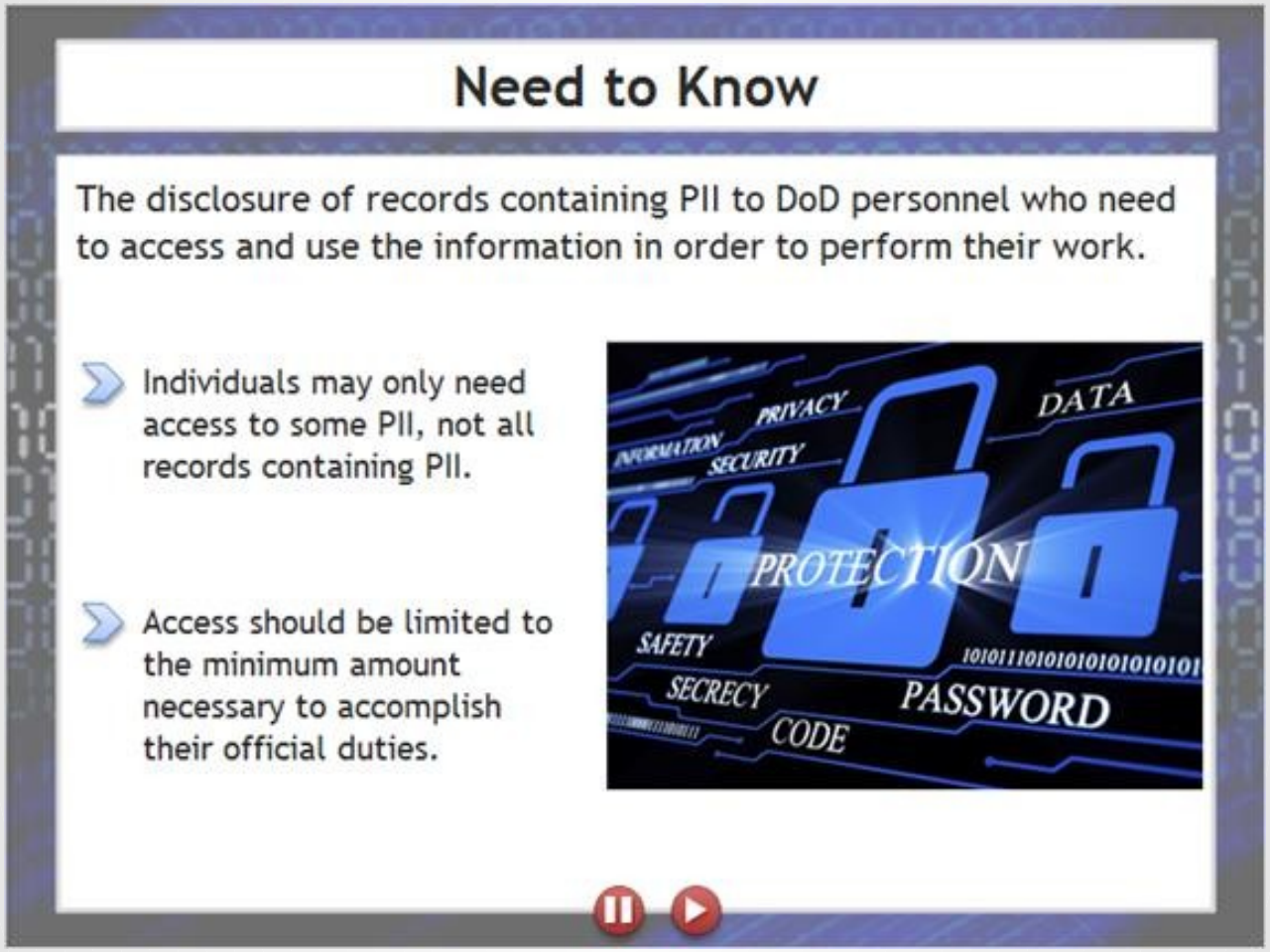
Captain Padlock: *Personally Identifiable Information (PII) is information used to distinguish or trace an individual's identity, such as name, social security number, mother's maiden name, and biometric records. PII can also include demographic, medical, and financial information, or any other information linked or linkable to a specific individual.*

3.4.2 System of Records (SOR)


System of Records (SOR)
A group of records under the control of a DoD Component from which personal information about an individual is retrieved by:
Name of the individual:
First Name:
Ann
Last Name:
Smith
Other unique identifier, such as a number or symbol:
Employee ID:
1088

Captain Padlock*:* System of Records. A group of records under the control of a DoD Component from which personal information about an individual is retrieved by the name of the individual, or by some other unique identifier, such as a number or symbol.

3.4.3 Need to Know


Need to Know
The disclosure of records containing PII to DoD personnel who need to access and use the information in order to perform their work.
Individuals may only need access to some PII, not all records containing PII.
Access should be limited to the minimum amount necessary to accomplish their official duties.
PRIVACY
DATA
INFORMATION
SECURITY
PROTECTION
SAFETY
SECRECY
PASSWORD
CODE

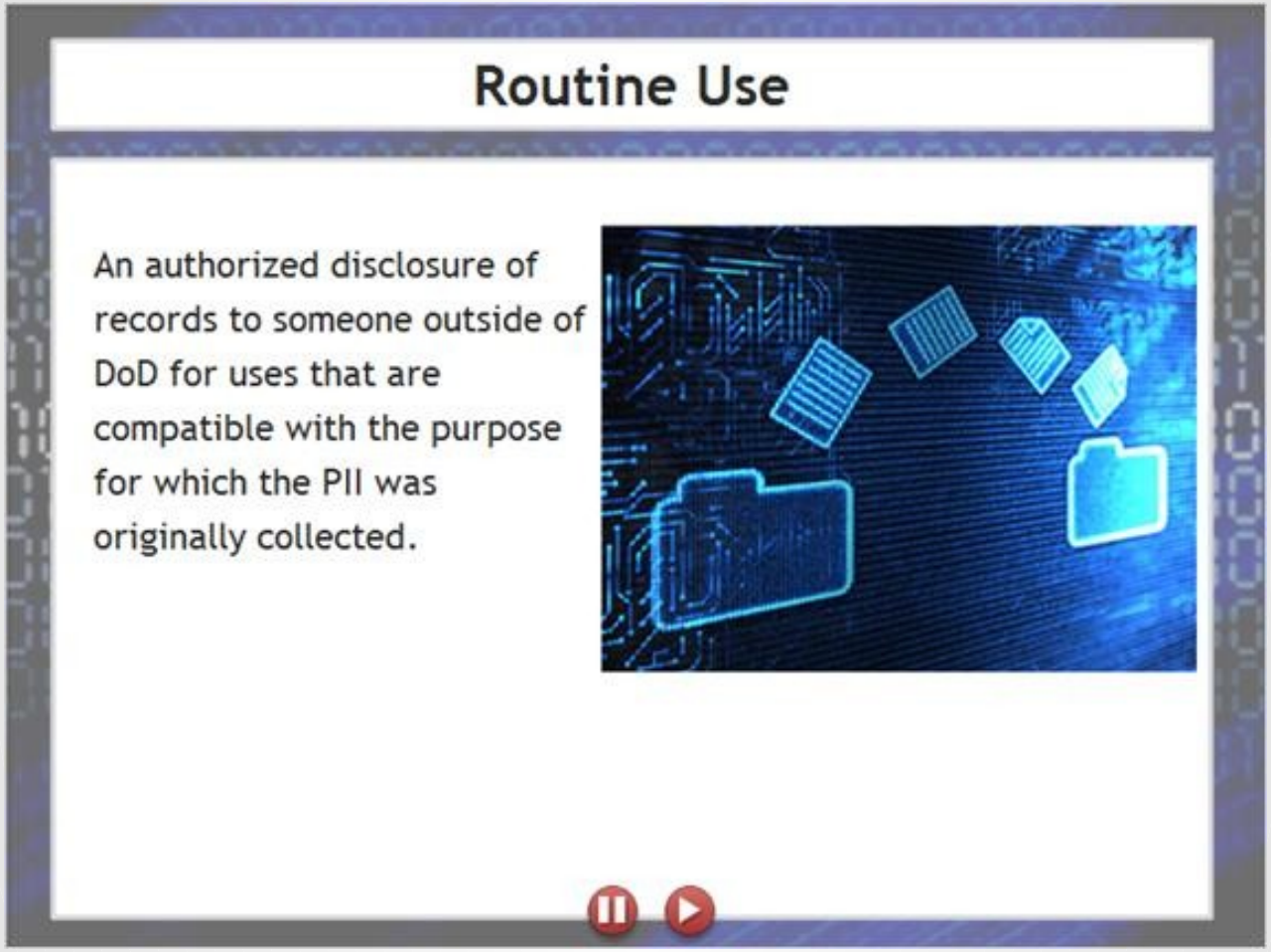
Captain Padlock: *Need to Know. The disclosure of records containing PII to DoD personnel who need to access and use the information in order to perform their work. However, even if an individual has a need to know some PII, that does not mean they should have access to all records containing PII. Access should be limited to the minimum amount necessary to accomplish their official duties.*

3.4.4 Safeguards

Privacy Safeguards
Safeguards are administrative, physical, or technical measures the Department takes to prevent unauthorized access to or disclosure of PII.
ADMINISTRATIVE
PRIVACY SAFEGUARDS
Administrative Safeguards - training personnel on information handling best practices
PHYSICAL
PRIVACY SAFEGUARDS
Physical Safeguards - Ensuring paper records and servers are secured and access is controlled
TECHNICAL
PRIVACY SAFEGUARDS
Technical Safeguards - encrypting computers and emails, and requiring Common Access Cards for system access

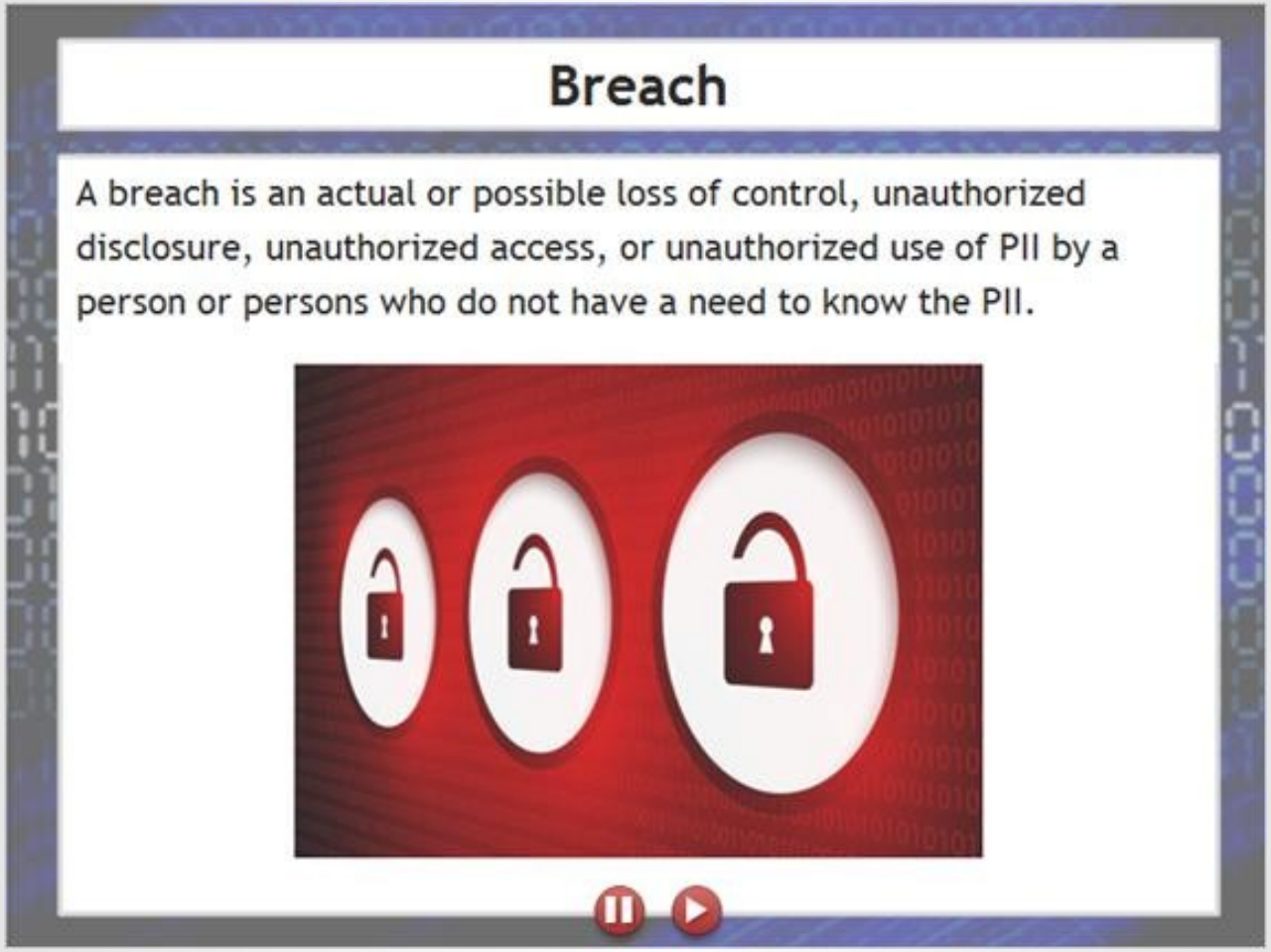
Captain Padlock: *Safeguards are administrative, physical, or technical measures the Department takes to prevent unauthorized access to or disclosure of PII.*

3.4.5 Routine Use


Routine Use
An authorized disclosure of records to someone outside of DoD for uses that are compatible with the purpose for which the PII was originally collected.

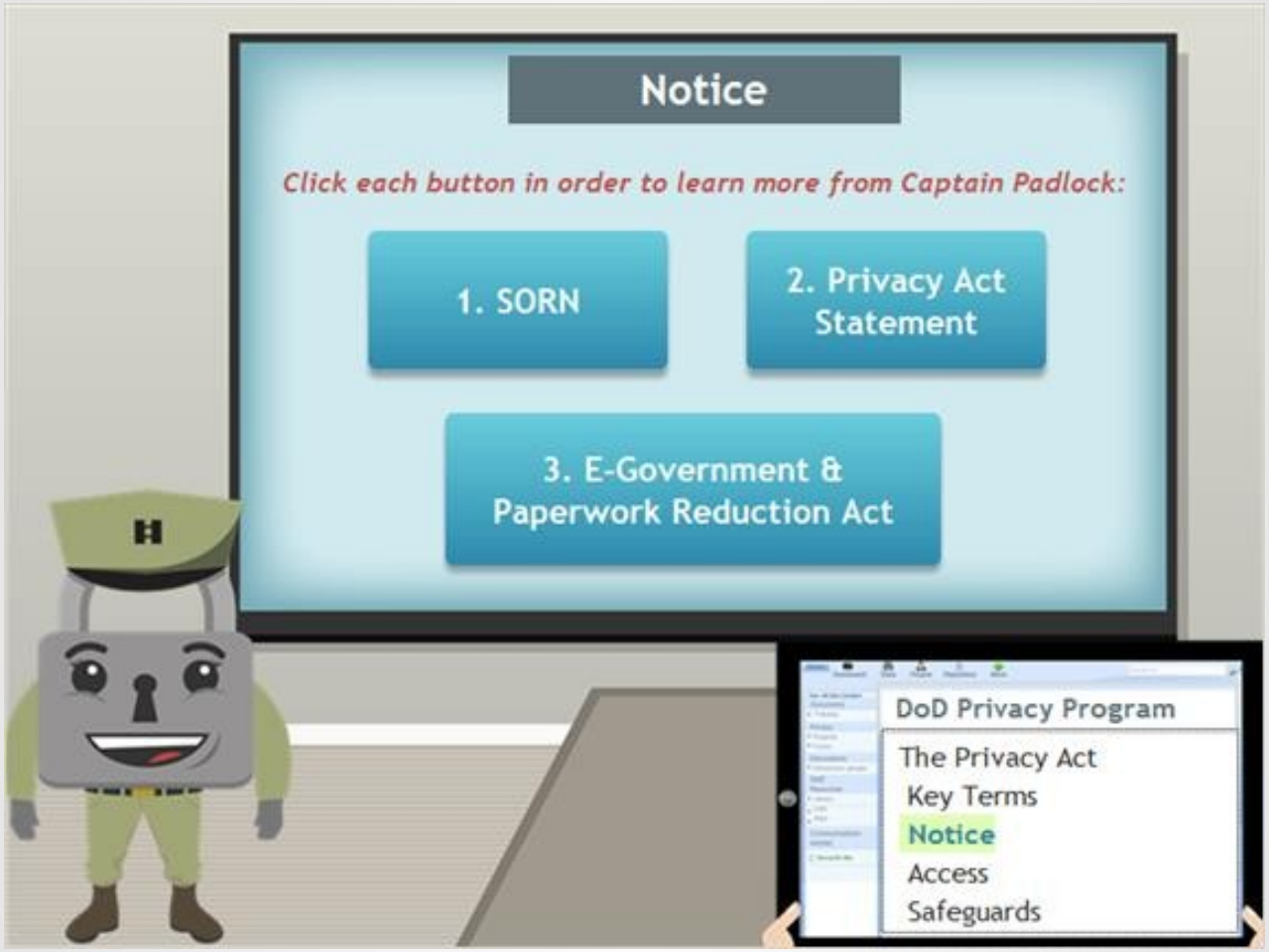
Captain Padlock: *Routine Use. An authorized disclosure of records to someone outside of DoD for uses that are compatible with the purpose for which the PII was originally collected.*

3.4.6 Breach


Breach
A breach is an actual or possible loss of control, unauthorized disclosure, unauthorized access, or unauthorized use of PII by a person or persons who do not have a need to know the PII.

Captain Padlock: *Breach. An actual or possible loss of control, unauthorized disclosure, unauthorized access, or unauthorized use of PII by a person or persons who do not have a need to know the PII.*

3.5 Notice: Inform Public



Captain Padlock: *Before the Department can collect any information from an individual for a system of records, it first must publish a System of Records Notice, or SORN in the Federal Register.*

3.5.1 SORN

System of Records Notice (SORN)

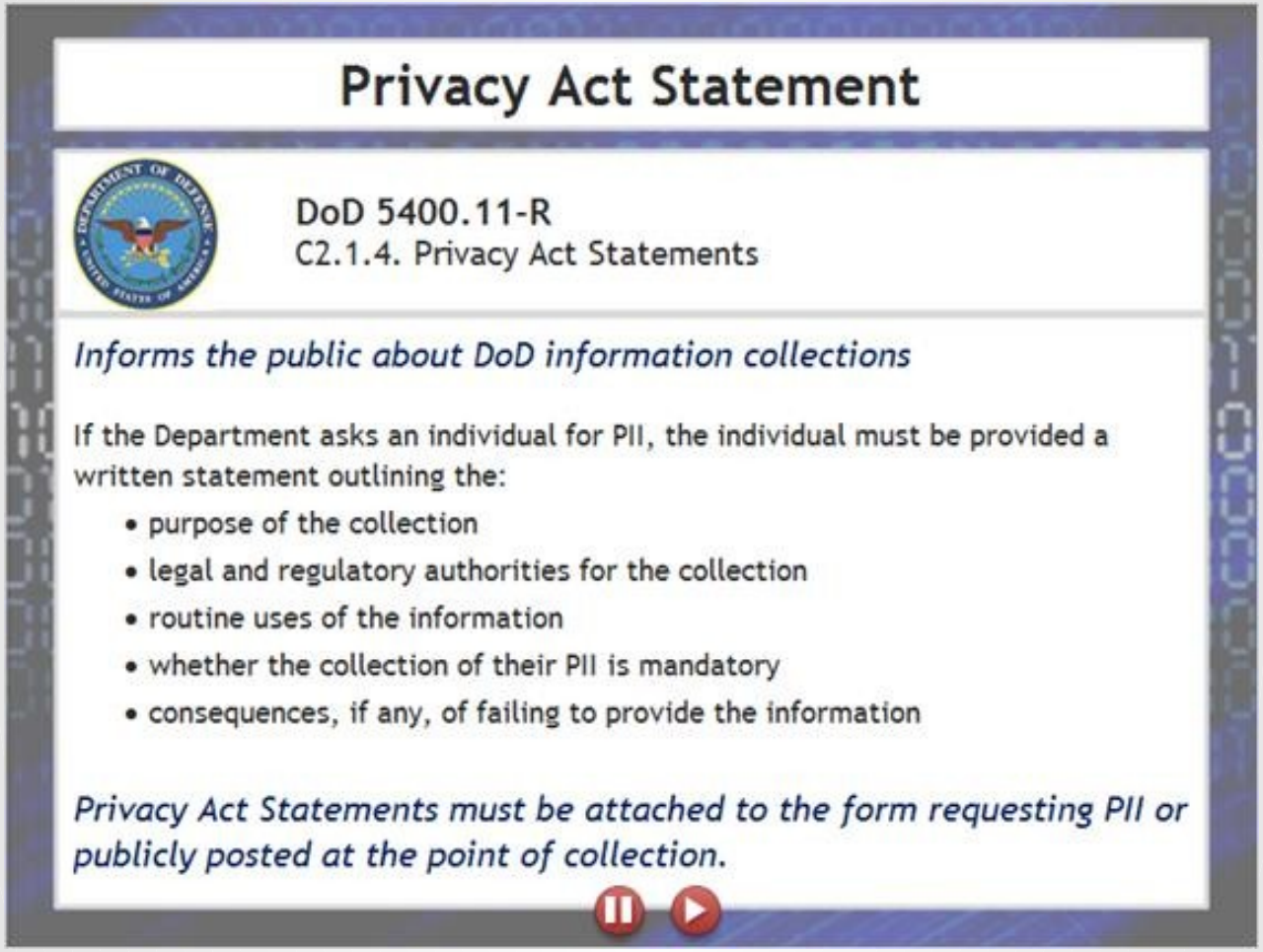
Notifies the public about the system of records including:

- categories of individuals
- categories of information
- purpose and authority for the collection
- record sources for the information collected
- any routine uses for the information
- how an individual may request access or amendment to their records

Operating a system of records without a published SORN is illegal, and can lead to civil penalties against the Department.

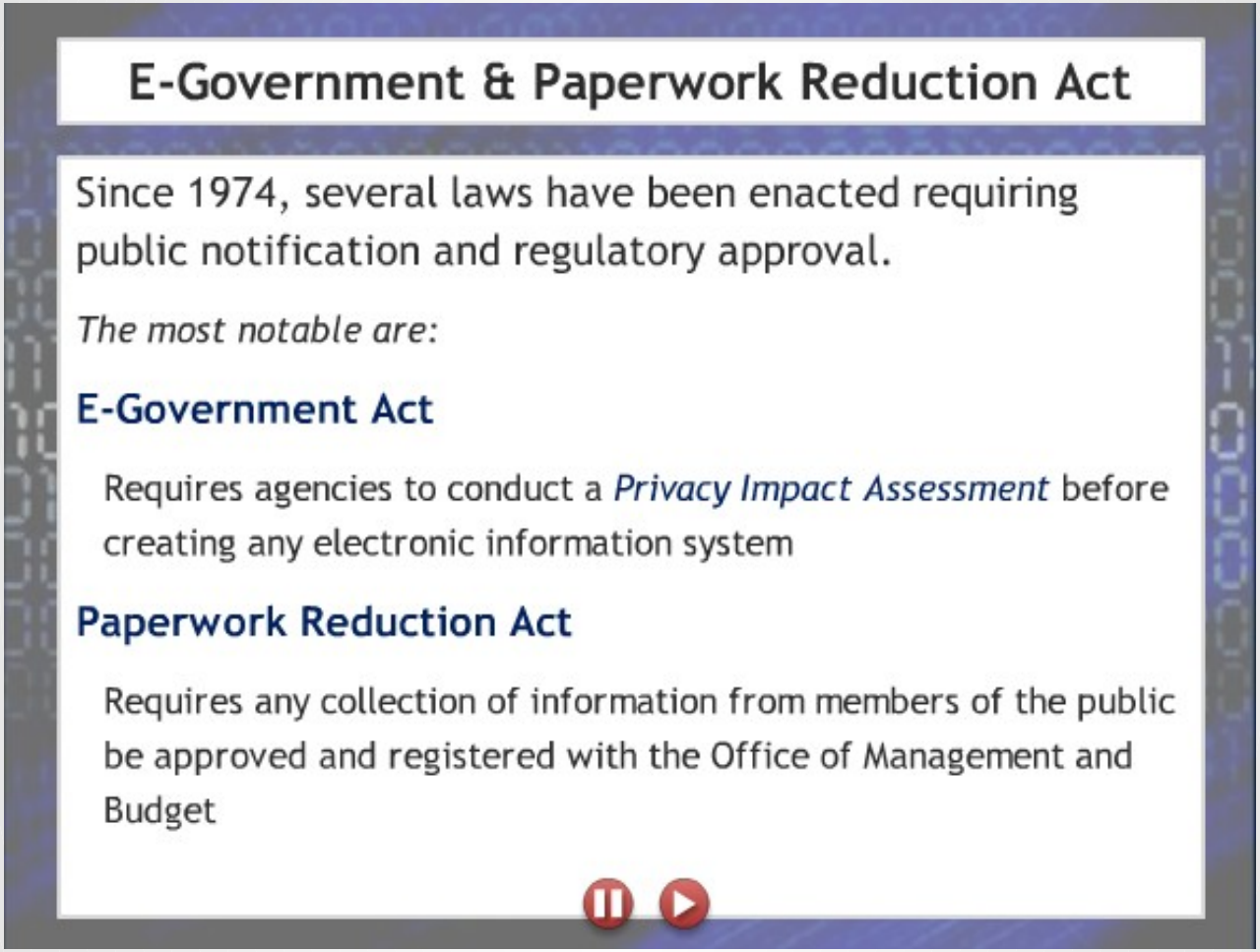
Captain Padlock: *A SORN notifies the public about the system of records; including the categories of individuals, the categories of information , the purpose and authority for the collection, the record sources for the information collected, any routine uses for the information, and how an individual may request access or amendment to their records. Operating a system of records without a published SORN is illegal, and can lead to civil penalties against the Department.*

3.5.2 Privacy Act Statement


Privacy Act Statement
DoD 5400.11-R
C2.1.4. Privacy Act Statements
Informs the public about DoD information collections
If the Department asks an individual for PII, the individual must be provided a written statement outlining the:
• purpose of the collection
• legal and regulatory authorities for the collection
• routine uses of the information
• whether the collection of their PII is mandatory
• consequences, if any, of failing to provide the information
Privacy Act Statements must be attached to the form requesting PII or publicly posted at the point of collection.

Captain Padlock: *A Privacy Act Statement is another way the Department informs the public about its information collections. Any time the Department asks an individual for PII, the individual must be provided a written statement outlining the purpose of the collection, the legal and regulatory authorities for the collection, the routine uses of the information, and whether the collection of their PII is mandatory, including the consequences, if any, of failing to provide the information. Privacy Act Statements must be attached to the form requesting PII or publicly posted at the point of collection.*

3.5.3 Privacy Laws


E-Government & Paperwork Reduction Act
Since 1974, several laws have been enacted requiring public notification and regulatory approval.
The most notable are:
E-Government Act
Requires agencies to conduct a Privacy Impact Assessment before creating any electronic information system
Paperwork Reduction Act
Requires any collection of information from members of the public be approved and registered with the Office of Management and Budget

***Captain Padlock**: Since 1974, several laws have been enacted requiring further means of public notification and regulatory approval. The most notable are the E-Government Act, which requires agencies to conduct a Privacy Impact Assessment before creating any electronic information system, and the Paperwork Reduction Act, which requires any collection of information from members of the public be approved and registered with the Office of Management and Budget.*

3.6 Notice Requirements

Captain Padlock: *You can learn more about these requirements by clicking on the links on your tablet now.*

3.7 Access: Individual Records

***Captain Padlock**: The Privacy Act requires the Department to ensure that the information it maintains is relevant, accurate, timely, and complete. While some records, such as law enforcement investigatory files, may be withheld, individuals generally are entitled to receive copies of records about themselves. The individual can also ask for a record to be amended if there are omissions or errors.*

3.8 Safeguards: Protect Information

***Captain Padlock**: The Privacy Act requires the Department to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual.*

3.9 InfoNet: Privacy Safeguards

Captain Padlock: *Click on the InfoNet screen now to see a sample of some of the Department's safeguards.*

3.10 Videos: Privacy Safeguards

Scene Description

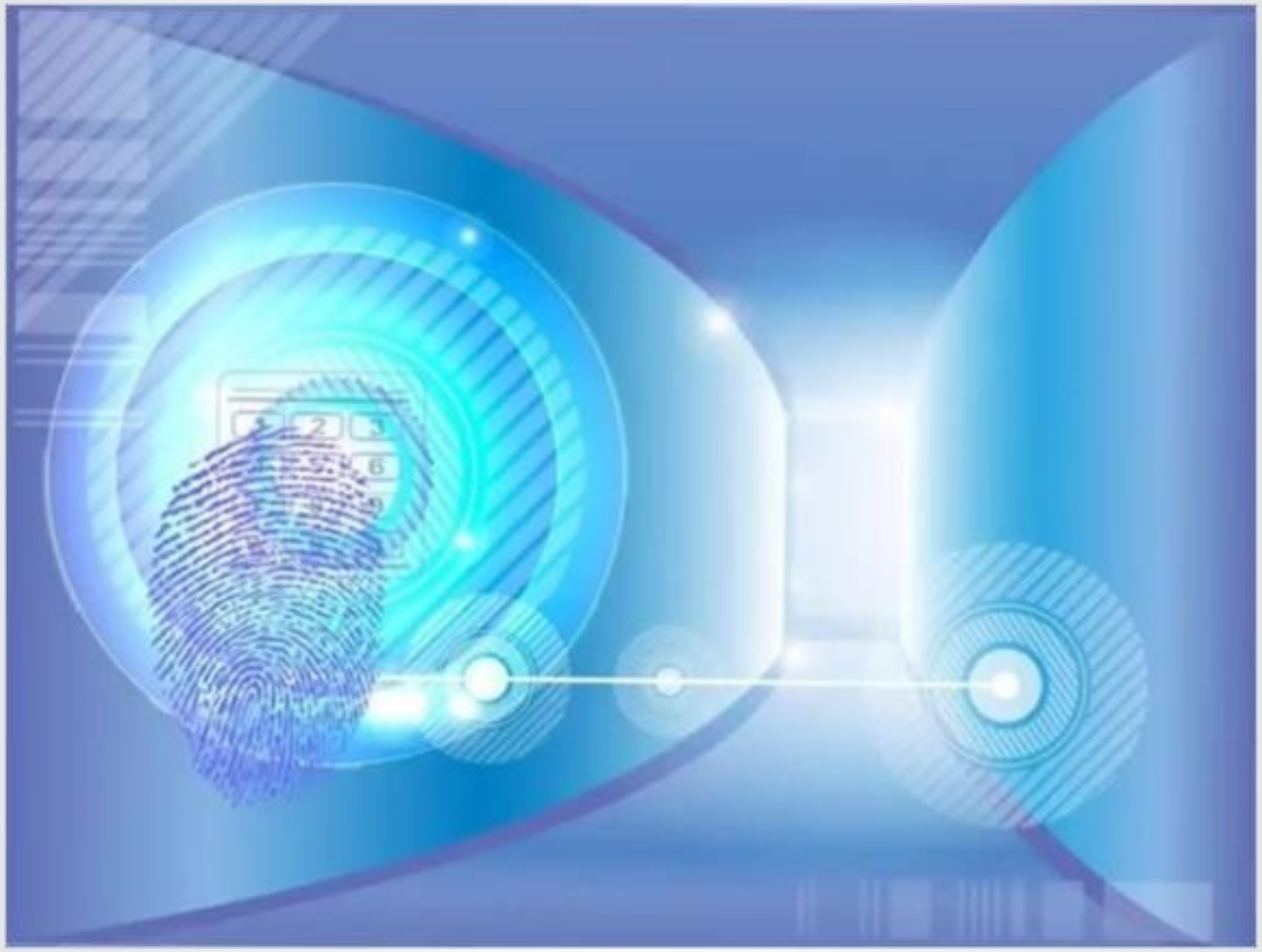
The InfoNet screen opens to view animated movies regarding Privacy Safeguards.

3.11 Bootcamp Completed

Captain Padlock: *I'm afraid that's all we have time to cover; we need you in the field ASAP! Before you go, you should know that your tablet doubles as a trans-time communications system. I'll be listening in throughout your mission and assisting in any way possible. If at any point you need my help, just click on my icon in the bottom left window. And don't worry, no one else can see or hear me but you. Now it's time for you to go back in time to stop this breach. Press ENERGIZE on your tablet to get started.*

Scene 4
First Time Travel: Remediation

4.1 Travel Back in Time - Remediation Goal



Scene Description

First Time Travel scene with a simulation effect of graphics, sound and movement.

4.2 SITREP: Remediation Status

Captain Padlock: *Changing the past can be a complicated and dangerous mission. From time to time TEMPCOM will send us a SITREP to show our progress in stopping this breach. Once the status bar is green we'll know we've accomplished our mission and normalized the timeline.*

Scene 5
System Development Meeting: Security Controls

5.1 System Requirements

SES: *Thank you all for your input. As we work on developing this new system to collect and store personal information on DoD personnel and their family members, I want to make sure that we're making it as efficient and secure as possible. So far we've talked about implementing administrative safeguards such as training staff on information handling practices, physical safeguards for ensuring servers and paper records are locked up and only accessible to authorized persons, and technical safeguards to encrypt computers and requiring Common Access Cards (CACs) for system access.*

5.1 System Requirements

SES: *If we take care of those requirements first, I think we'll have a pretty secure IT system. So if no one else has any concerns, I think we're almost ready to turn on the system and start collecting information! Oh, Private C, I didn't see you come in. Can you think of anything else that we need to do first?*

Captain Padlock: *It sounds to me like they may be missing some of the required privacy processes for setting up a system to collect PII. Tell them what they're missing.*

5.2 Knowledge Check 1: Secure System

Correct Answer

SORN, PIA and OMB Approval for PRA

Captain Padlock: *A system collecting and retrieving PII must have a System of Records Notice to comply with the Privacy Act. An IT system must also have a Privacy Impact Assessment to comply with the E-Government Act. Finally, the Office of Management and Budget must approve all collections from members of the public to comply with the Paperwork Reduction Act.*

5.3 System Privacy Compliance

SES: *I'm very glad you brought those matters to our attention; we'll have to start working on our privacy compliance right away! Suzie, get in touch with our Information Management Control Officer to discuss Paperwork Reduction Act requirements. Jake, call our Privacy Officer to get the SORN process started. I'll make sure our PIA is in order.*

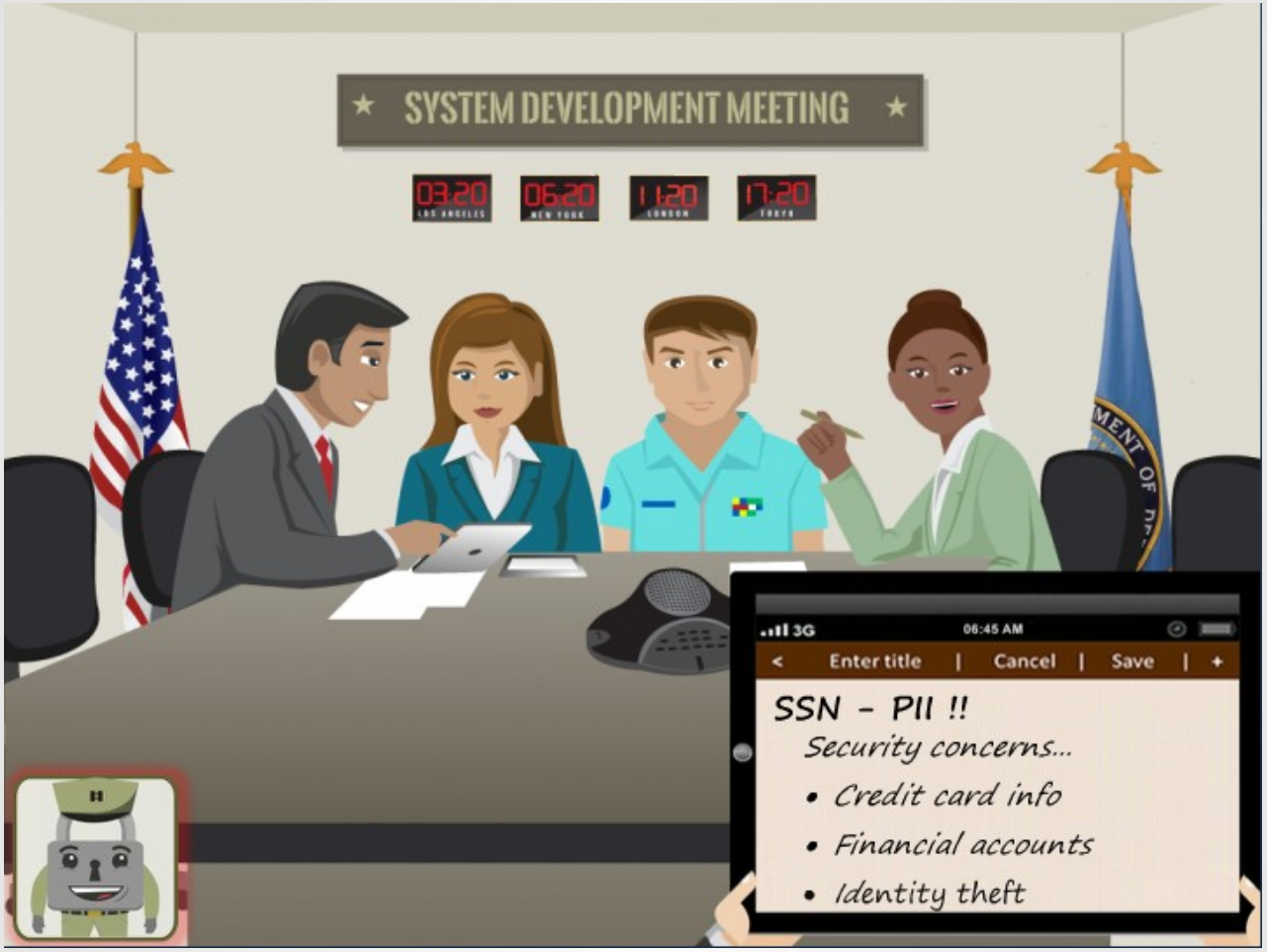
5.3 System Privacy Compliance

SYSTEM DEVELOPMENT MEETING
03:20
06:20
11:20
17:20
Department of Defense
INSTRUCTION
NUMBER 1000.30
August 1, 2012
USD(P&R)
SUBJECT: Reduction of Social Security Number (SSN) Use Within DoD
References: See Enclosure 1
1. PURPOSE. This Instruction:
a. Establishes policy and assigns responsibilities for SSN use reduction in the Department of Defense in accordance with the authority in DoD Directive 5124.02 (Reference (a)).
b. Establishes a DoD SSN Use Reduction Plan.

Suzie: *There's one more question. We've been trying to figure out the best way to uniquely identify people with similar names. I think the easiest thing would be for us to just use their Social Security Numbers. I know we weren't planning on collecting them, and we don't need them for anything else, but I figure everyone knows their SSN, so we can just use them for all of our records.*

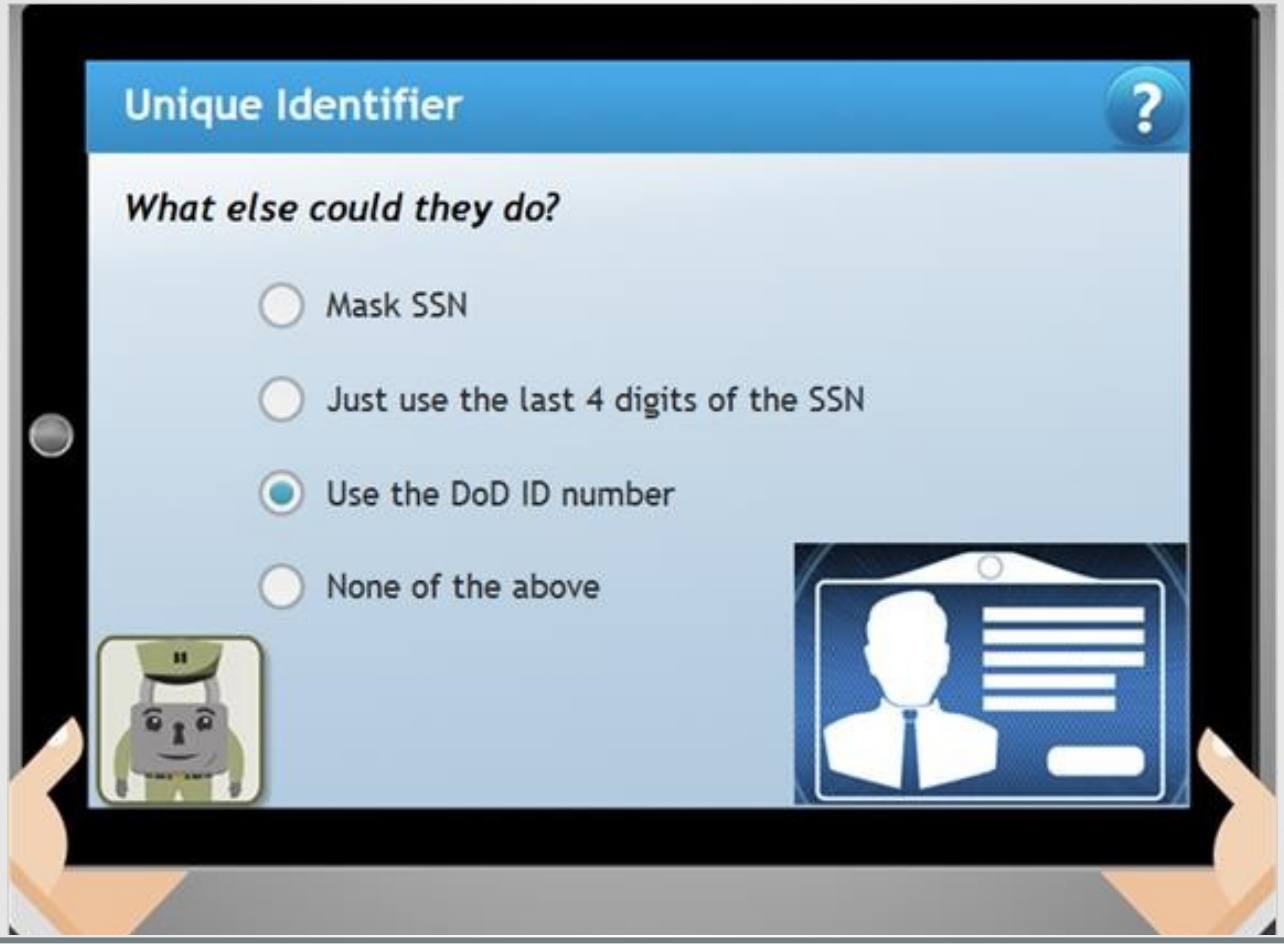
SES: *I guess that makes sense. What do you think, Private C?*

5.3 System Privacy Compliance



Captain Padlock: *Good Grief! Social Security Numbers are some of the most valuable pieces of PII there are. With just an SSN and a little biographical information, identity thieves can obtain credit cards, access your financial accounts, or even impersonate you! Tell them about another option that is safer.*

5.4 Knowledge Check 2: Unique ID


Unique Identifier
What else could they do?
Mask SSN
Just use the last 4 digits of the SSN
Use the DoD ID number
None of the above

Correct Answer

Use the DOD ID number

***Captain Padlock**: While masking Social Security Numbers or using only the final 4 digits are both prudent methods of protecting SSNs, they should only be used in secure systems that require the SSN for an authorized purpose. Systems like this one, which don't need the SSN, shouldn't collect it at all. For most systems, an alternate identifier can be substituted for the SSN. That's why the Department introduced the DoD ID Number to uniquely identify individuals affiliated with the Department.*

5.5 Meeting Summary

SES: *You know, come to think of it, I remember going to a meeting about the new DoD ID Number. It's completely unique, and everyone affiliated with the DoD has one that stays with them for life. Best of all, it has no value to identity thieves. We should definitely use that instead. Well, we all know what we need to do now to ensure our system has the appropriate privacy controls and documentation in place. Thanks for your help, Private C.*

5.5 Time Travel Energize

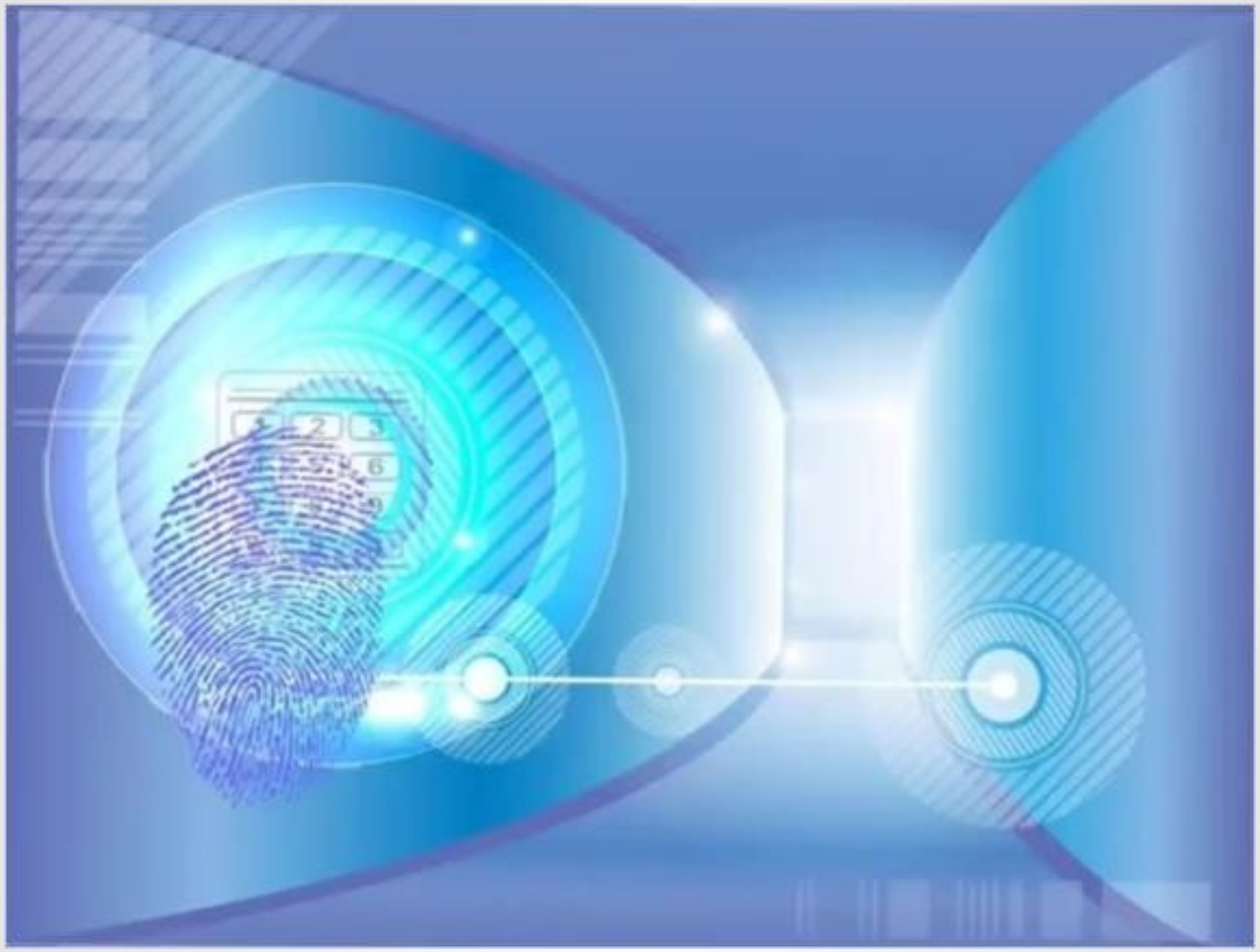
Captain Padlock: *Good work, but TEMPCOM indicates that the breach will still occur. We'll have to jump to another time to make sure we can stop it.*

Scene 6

Second Time Travel:

Physical Safeguards

6.1 Travel Back in Time: Hacker Attack



Scene Description

Second Time Travel scene with a simulation effect of graphics, sound and movement.

6.2 SITREP: Physical Safeguards

Captain Padlock: *Oh no! Someone's trying to hack into TEMPCOM. It must be the criminals involved in the breach, trying to keep you from succeeding. Help us set up physical safeguards to ensure we can keep them out!*

6.3 Knowledge Check 1: Offices

ALERT! Hacker Attack in Progress!
Physical Safeguards
?
Answer True or False:
1. Offices and installations that maintain or process PII should always have door locks and access control systems to prevent unauthorized access.
True
False

Correct Answer

True: Offices and installations that maintain or process PII should always have door locks and access control systems to prevent unauthorized access.

6.4 Knowledge Check 2: Documents

ALERT! Hacker Attack in Progress!
Physical Safeguards
?
Answer True or False:
2. When not in use, documents and media containing PII should be kept in a locked cabinet.
True
False

Correct Answer

True: When not in use, documents and media containing PII should be kept in a locked cabinet.

6.5 Knowledge Check 3: Laptops

ALERT! Hacker Attack in Progress!
Physical Safeguards
?
Answer True or False:
3. Locking your computer in your car while you run errands is a sufficient physical safeguard.
True
False

Correct Answer

False: Locking your computer in your car while you run errands is a sufficient physical safeguard.

Scene 7
Waiting Room: Data Collection

7.1 Waiting Room: Forms with PII

Clerk: *Mr. Breached, thank you for coming in today. I'd be happy to get you registered in our system. I just need your completed DD Form 387-B. Oh, it looks like you filled out the DD Form 387-A by mistake. It's ok, I'll help you fill out the* correct form. Oh, Private C, I didn't see you come in. Can you dispose of this form with Mr. Breached's information for me?

7.2 Knowledge Check 1: Disposal

Captain Padlock: **Trash Can** - Wait! That form has Personally Identifiable Information on it! PII needs to be disposed of in a manner that makes it unrecognizable and beyond reconstruction. For paper records, that generally means burning. **Recycling Bin** - Wait! While I can appreciate your sense of environmentalism, that form has Personally Identifiable Information on it! PII needs to be disposed of in a manner that makes it unrecognizable and beyond reconstruction. For paper records, that generally means burning. **Burn Bag** - Good choice! Records containing someone's Personally Identifiable Information must always be disposed of in a manner that makes it unrecognizable and beyond reconstruction. For paper records, that generally means burning.

7.3 SSN and Other PII

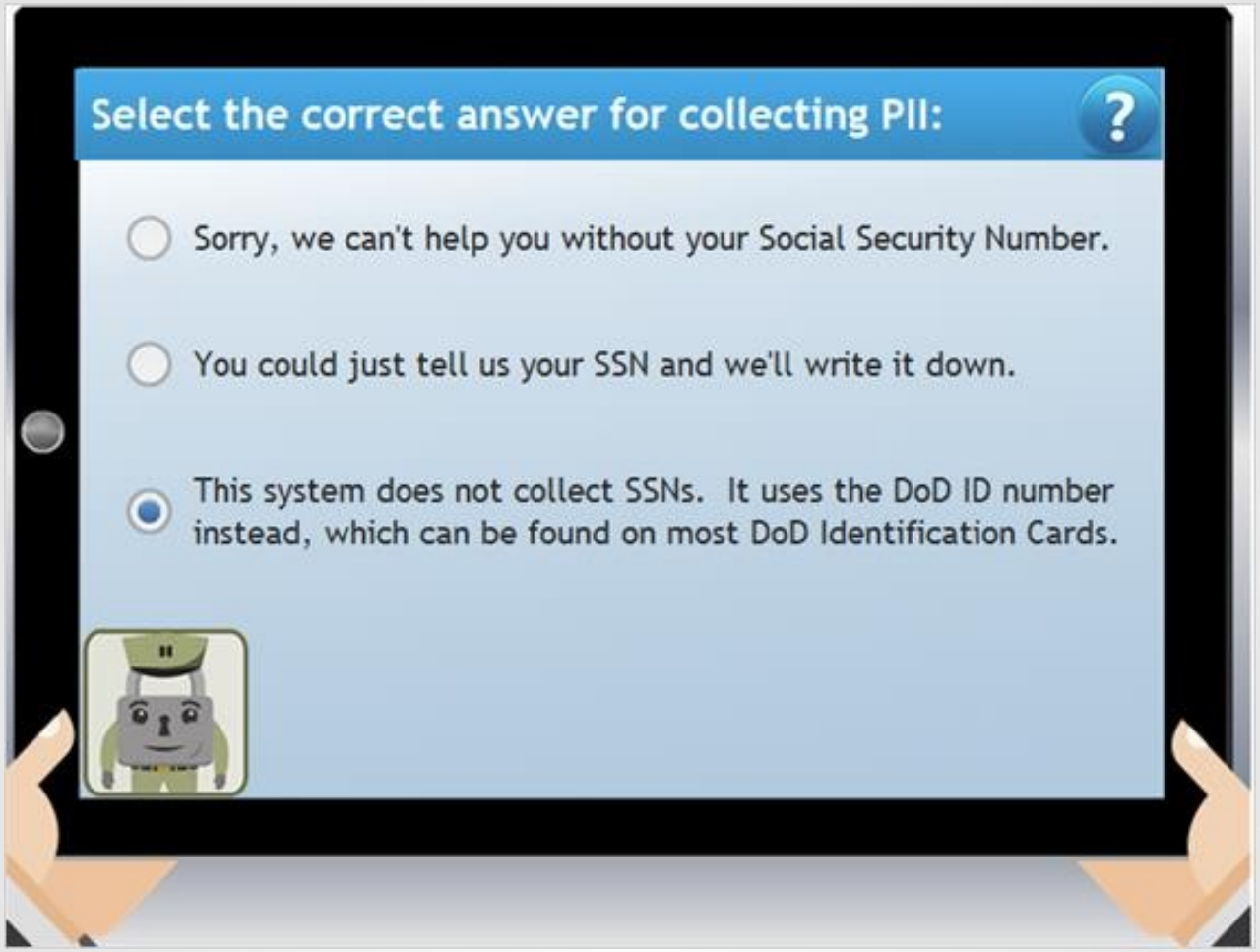
Clerk: *Ok, I just need your name, the names of your family members, your address, phone number, date of birth, mother's maiden name, your bank account routing number, and two forms of ID, one of which has to have your Social Security Number on it.*

7.3 SSN and Other PII

Ben Breached: *Oh, um, I didn't bring my social security card. Is there something else I can use?*

Clerk: *Well, we usually use it just to make sure you are who you say you are… Private C, do you know of any alternatives?*

7.4 Knowledge Check 2: Collecting PII


Select the correct answer for collecting PII:
Sorry, we can't help you without your Social Security Number.
You could just tell us your SSN and we'll write it down.
This system does not collect SSNs. It uses the DoD ID number instead, which can be found on most DoD Identification Cards.

Correct Answer

This system does not collect SSNs. It uses the DoD ID number instead, which can be found on most DoD Identification Cards.

7.5 Privacy Act Statement

Clerk: *Oh I didn't know we weren't supposed to collect the SSN in this system. From now on I'll only ask for the DoD ID number.*
Ben Breached: *You know, this really is an awful lot of personal information you're taking down. Is there some way for me to know everything that you plan on doing with it?*
Clerk: *Umm, I'm really not sure. Private C, do you know?*

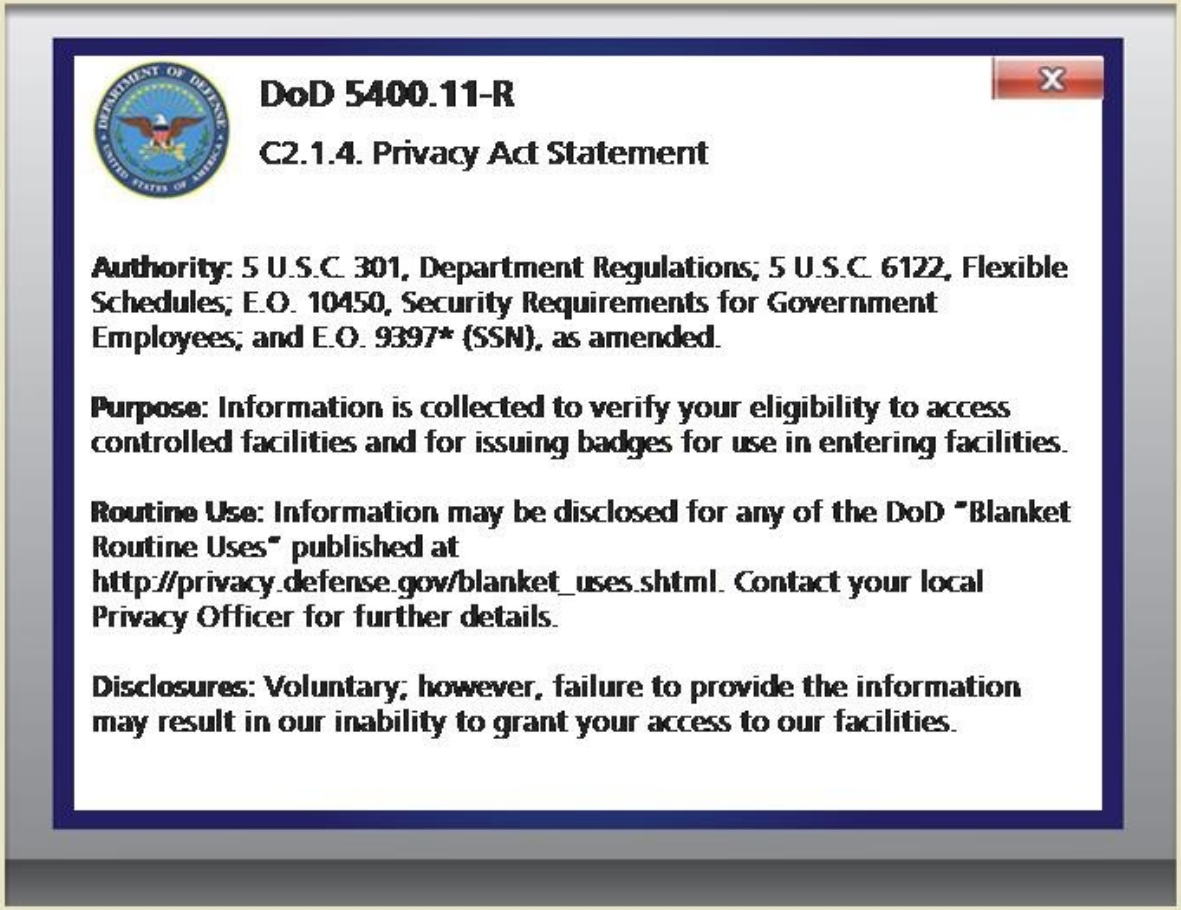
7.5 Privacy Act Statement

Captain Padlock: *Under the Privacy Act, that kind of information has to be presented to the individual at the point of collection of his or her PII. Do you see anything like that posted here?*

…

Excellent job! That's a Privacy Act Statement.

7.5 Privacy Act Statement


DoD 5400.11-R
C2.1.4. Privacy Act Statement
Authority: 5 U.S.C. 301, Department Regulations; 5 U.S.C. 6122, Flexible Schedules; E.O. 10450, Security Requirements for Government Employees; and E.O. 9397* (SSN), as amended.
Purpose: Information is collected to verify your eligibility to access controlled facilities and for issuing badges for use in entering facilities.
Routine Use: Information may be disclosed for any of the DoD "Blanket Routine Uses" published at http://privacy.defense.gov/blanket_uses.shtml. Contact your local Privacy Officer for further details.
Disclosures: Voluntary; however, failure to provide the information may result in our inability to grant your access to our facilities.

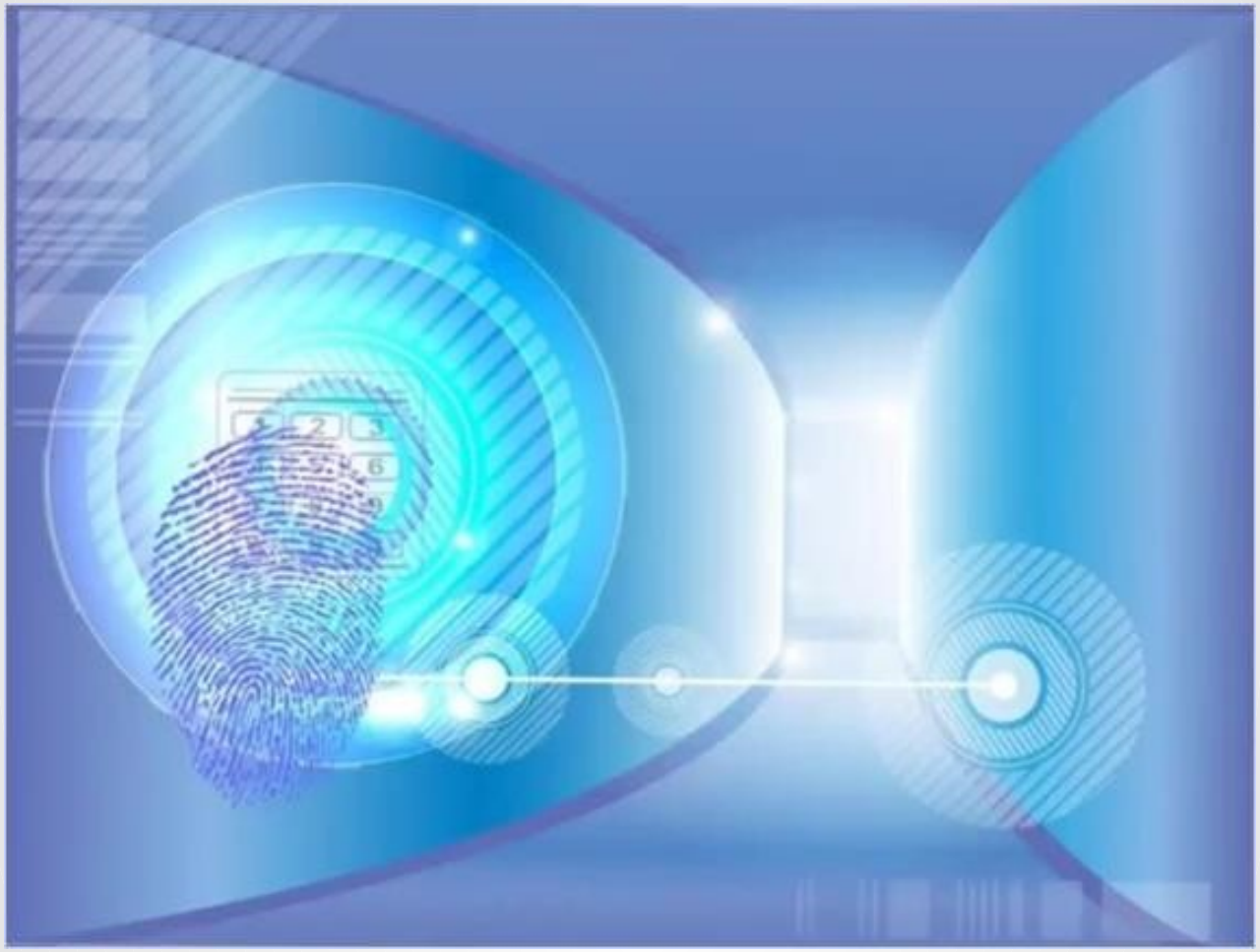
***Captain Padlock**: A Privacy Act Statement is required whenever PII is collected from an individual. It tells the individual the purpose of the collection, the legal and regulatory authorities for the collection, the routine uses of the information, and whether or not the collection of their PII is voluntary or mandatory, including the consequences, if any, of failing to provide the information. Privacy Act Statements must be included on all forms collecting PII for a system of records or can be posted anywhere such information is routinely collected. If requested, a printed copy of the Privacy Act Statement must be made available to the individual.*

7.6 Collection & Disposal Resolved

Captain Padlock: *I think we've done all we can do here, but TEMPCOM is telling me that the breach will still happen! We'll have to jump forward to see if we can fix a few other problems.*

Scene 8
Third Time Travel:
Administrative Safeguards

8.1 Travel Back in Time: Hacker Attack



Scene Description

Third Time Travel scene with a simulation effect of graphics, sound and movement.

8.2 SITREP: Administrative Safeguards

Captain Padlock: *Oh No! Those hackers are back at it. Quick, help us set up administrative safeguards to ensure we can keep them out!*

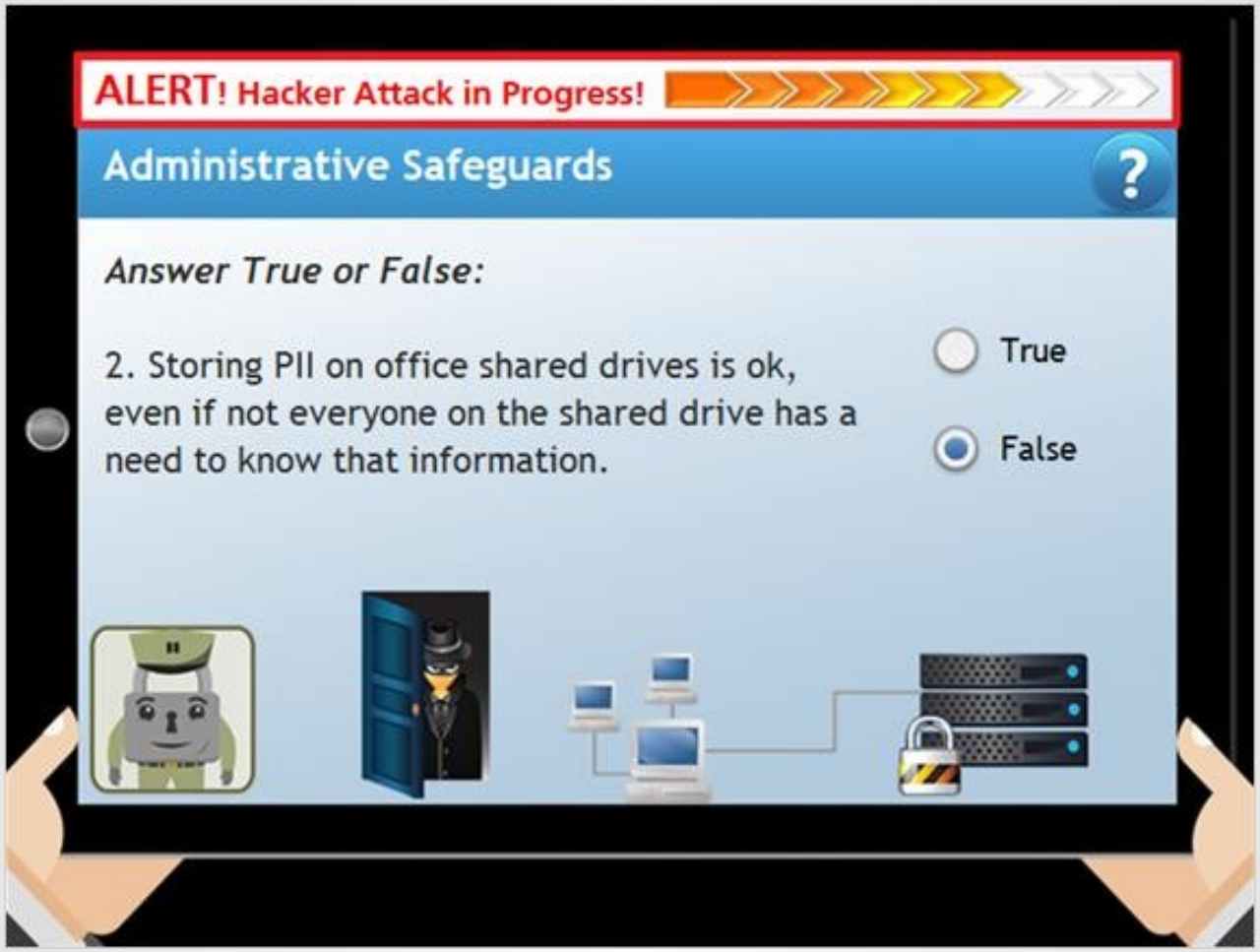
8.3 Knowledge Check 1: Breach

ALERT! Hacker Attack in Progress!
Administrative Safeguards
Answer True or False:
1. If you discover a breach, you must report it to your component privacy officer immediately.
True
False

Correct Answer

True: If you discover a breach, you must report it to your component privacy officer immediately.

8.4 Knowledge Check 2: Need to Know


ALERT! Hacker Attack in Progress!
Administrative Safeguards
?
Answer True or False:
2. Storing PII on office shared drives is ok, even if not everyone on the shared drive has a need to know that information.
True
False

Correct Answer

False: Storing PII on office shared drives is ok, even if not everyone on the shared drive has a need to know that information.

8.5 Knowledge Check 3: Workforce Training

Correct Answer

True: Any person who handles PII must take annual privacy training.

Scene 9
Office Cubicle: Maintenance

9.1 Disclosing PII

Tom: *Hey Jim! How's it going… Nah, I'm just toiling away, you know, nose to the grindstone. Actually, I'm working on the file of this guy who lives in your building. You probably know him.*

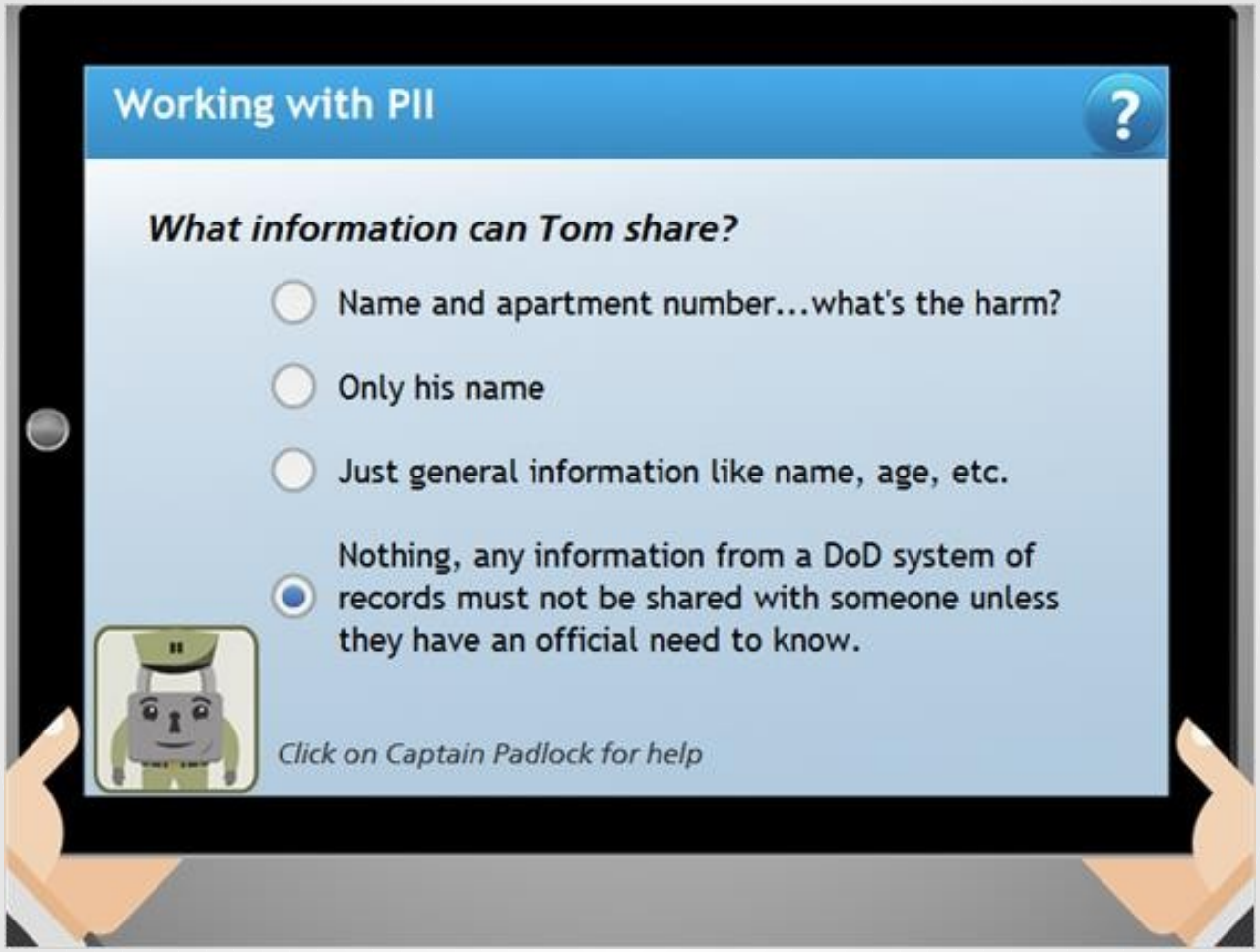
Jim, hold on a second.

9.2 Need to Know

Tom: *Oh, hey Private C, I didn't see you come in. I was just talking to my buddy Jim. Can you believe this guy Ben Breached lives right down the hall from him? Jim's new in town, and maybe he and this Ben guy could hang out.*

Captain Padlock: *I'm not sure Tom should be sharing this information with someone who doesn't have a need to know. Make sure he doesn't cause a breach.*

9.3 Knowledge Check 1: Sharing PII


Working with PII
?
What information can Tom share?
Name and apartment number...what's the harm?
Only his name
Just general information like name, age, etc.
Nothing, any information from a DoD system of records must not be shared with someone unless they have an official need to know.
Click on Captain Padlock for help

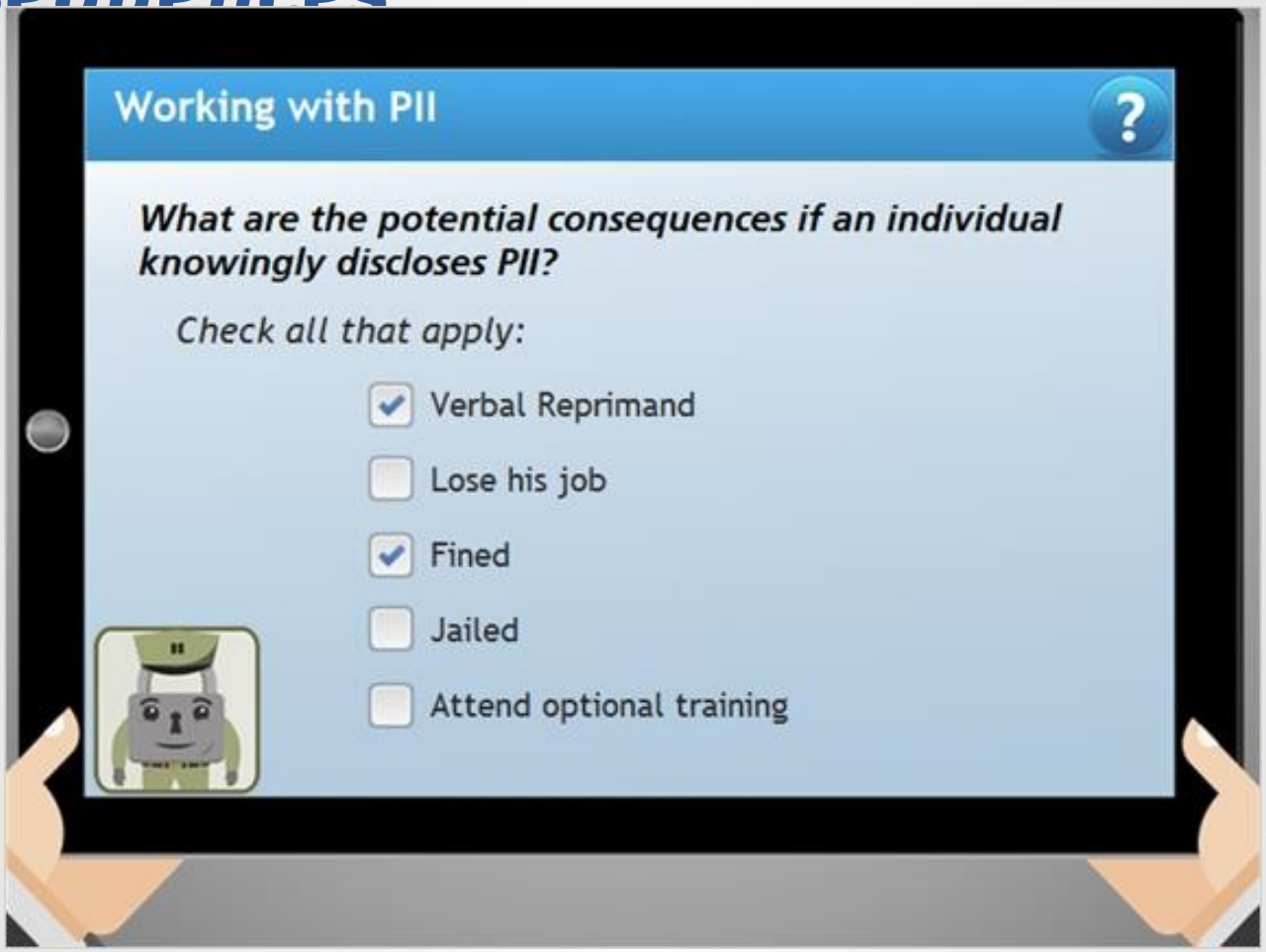
Correct Answer
Nothing, any information from a DoD system of records must not be shared with someone unless they have an official need to know.
Captain Padlock: *Personal information collected or stored in a system of records by the Department should never be shared with anyone who doesn't have a need to know. Even seemingly harmless information can hurt an individual if improperly disclosed. AND, it's a violation of the Privacy Act.*

9.4 Causing a Breach

Tom: *Never mind Jim, I guess I really shouldn't be talking about it.* (Wah wah wah) *Oh I'm sorry to hear that your divorce isn't going well.* (Wah wah?) *Well, I do have access to your ex-wife's files, but I don't know if I'm allowed to share them with you. I guess I could help you out, just this once.*

Captain Padlock: *It sounds like Tom is about to knowingly violate the Privacy Act. Tell him what might happen if he knowingly discloses this information.*

9.5 Knowledge Check 2: Consequences



Correct Answer
Verbal Reprimand and Fined
Captain Padlock: *If a Service member, civilian employee or DoD contractor accidentally discloses information incorrectly, the Privacy Act allows the Department to take administrative actions such as reprimands or retraining. But if a service member, civilian employee or DoD contractor knowingly and willfully violates the law, it can lead to civil suits against the Department and criminal charges resulting in fines for the individual.*

9.6 Take Work Home

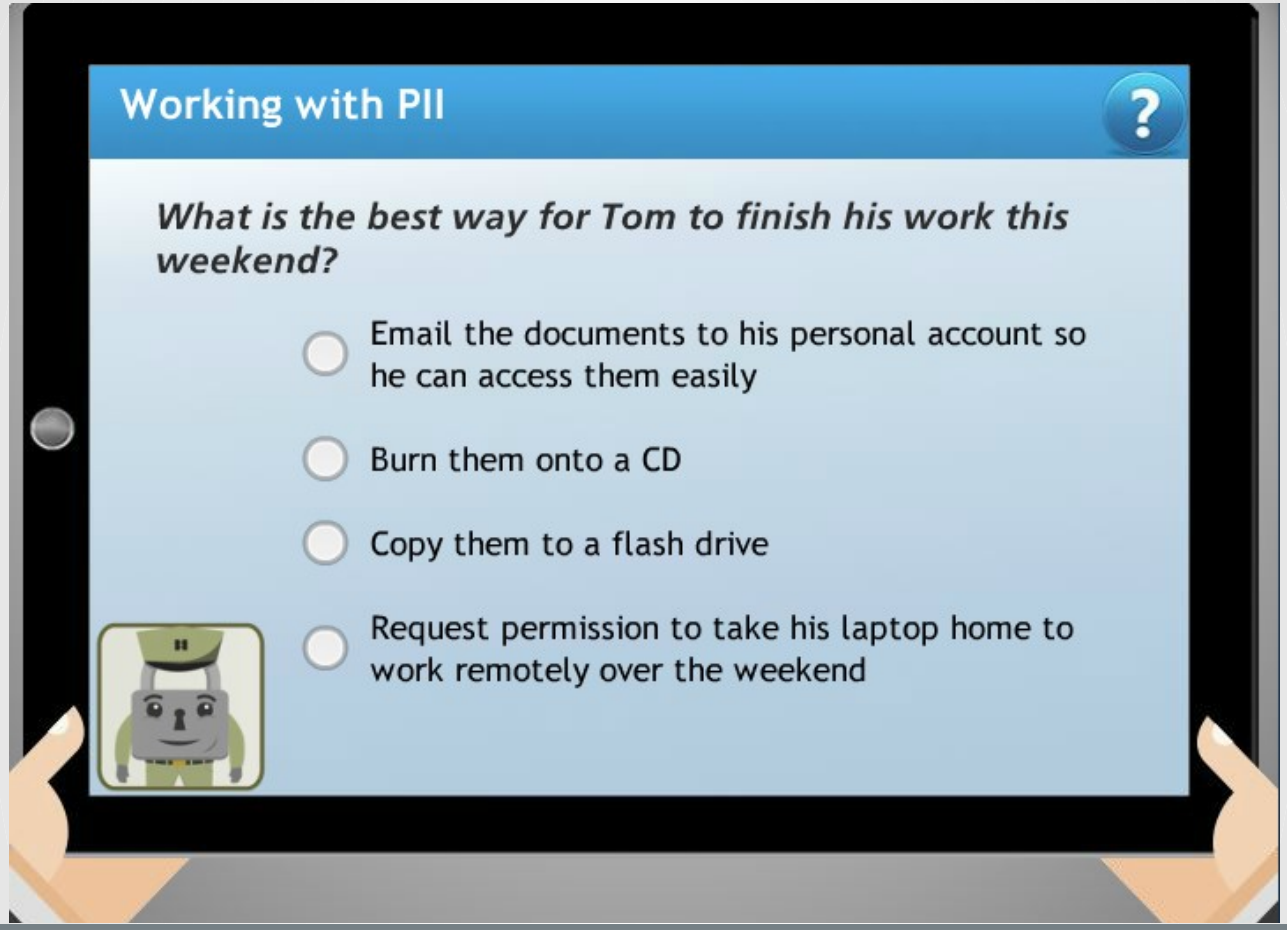
Tom: *I didn't know it was that serious… I'm sorry Jim, I just can't do that.*

9.6 Take Work Home

Tom: Oh man! It's already 4:30!? I finally get a date with Jenny, and now I'm going to be late! I didn't even have time to finish up my work for the day. Oh man, my director is gonna be furious. I guess I'll just have to take these files home and finish them over the weekend.

Captain Padlock*:* Taking work out of the office can lead to a loss of control of the information an employee is working on. If he has to work on these records over the weekend, make sure he does it the right way.

9.6 Knowledge Check 3: Telework


Working with PII
?
What is the best way for Tom to finish his work this weekend?
Email the documents to his personal account so he can access them easily
Burn them onto a CD
Copy them to a flash drive
Request permission to take his laptop home to work remotely over the weekend

Correct Answer
Request permission to take his laptop home to work remotely
Captain Padlock: *That's right, transmitting PII over unsecured networks, such as personal email accounts, is a breach of that information and has to be reported. Rewritable media, such as CDs and flash drives, can also pose a risk to information as they can easily be lost and may even contain viruses that could compromise a work station. You should always leave PII on official, DoD-approved hardware and networks to avoid its compromise. When teleworking, you should never leave your work computer or handheld device unattended in public, even if it's locked in your car.*

9.7 Telework

Tom: *I hadn't thought about the risks associated with using removable storage devices or emailing my work for use at home. I guess I should go ask my boss if I can telework and take my computer home.*

Captain Padlock: *Great work! But TEMPCOM says there's still a 25 percent chance the breach will still occur. We need to jump to one more temporal distortion to stop this breach for*

Scene 10

Fourth Time Travel:

Technical Safeguards

10.1 Travel Back in Time: Hacker Attack

Scene Description
Fourth Time Travel screen with a simulation effect of graphics, sound and movement.

10.2 SITREP: Technical Safeguards

Captain Padlock: *Oh No! Those hackers are back at it. Quick, help us set up technical safeguards to ensure we can keep them out!*

10.3 Knowledge Check 1: Encryption

ALERT! Hacker Attack in Progress!
Technical Safeguards
?
Answer True or False:
1. It's ok to use un-encrypted computers for documents with PII if you don't have access to your regular computer.
True
False

Correct Answer

False: It's ok to use un-encrypted computers for documents with PII if you don't have access to your regular computer.

10.4 Knowledge Check 2: Locks & Passwords

ALERT! Hacker Attack in Progress!
Technical Safeguards
?
Answer True or False:
2. Computers that process PII should be equipped with an automatic time-out feature that locks the system and requires password re-entry.
True
False

Correct Answer

True: Computers that process PII should be equipped with an automatic time-out feature that locks the system and requires password re-entry.

10.5 Knowledge Check 3: Encrypted Emails

ALERT! Hacker Attack in Progress!
Technical Safeguards
?
Answer True or False:
3. Emails with PII don't need to be encrypted if they aren't leaving the Department.
True
False

Correct Answer

False: Emails with PII don't need to be encrypted if they aren't leaving the Department.

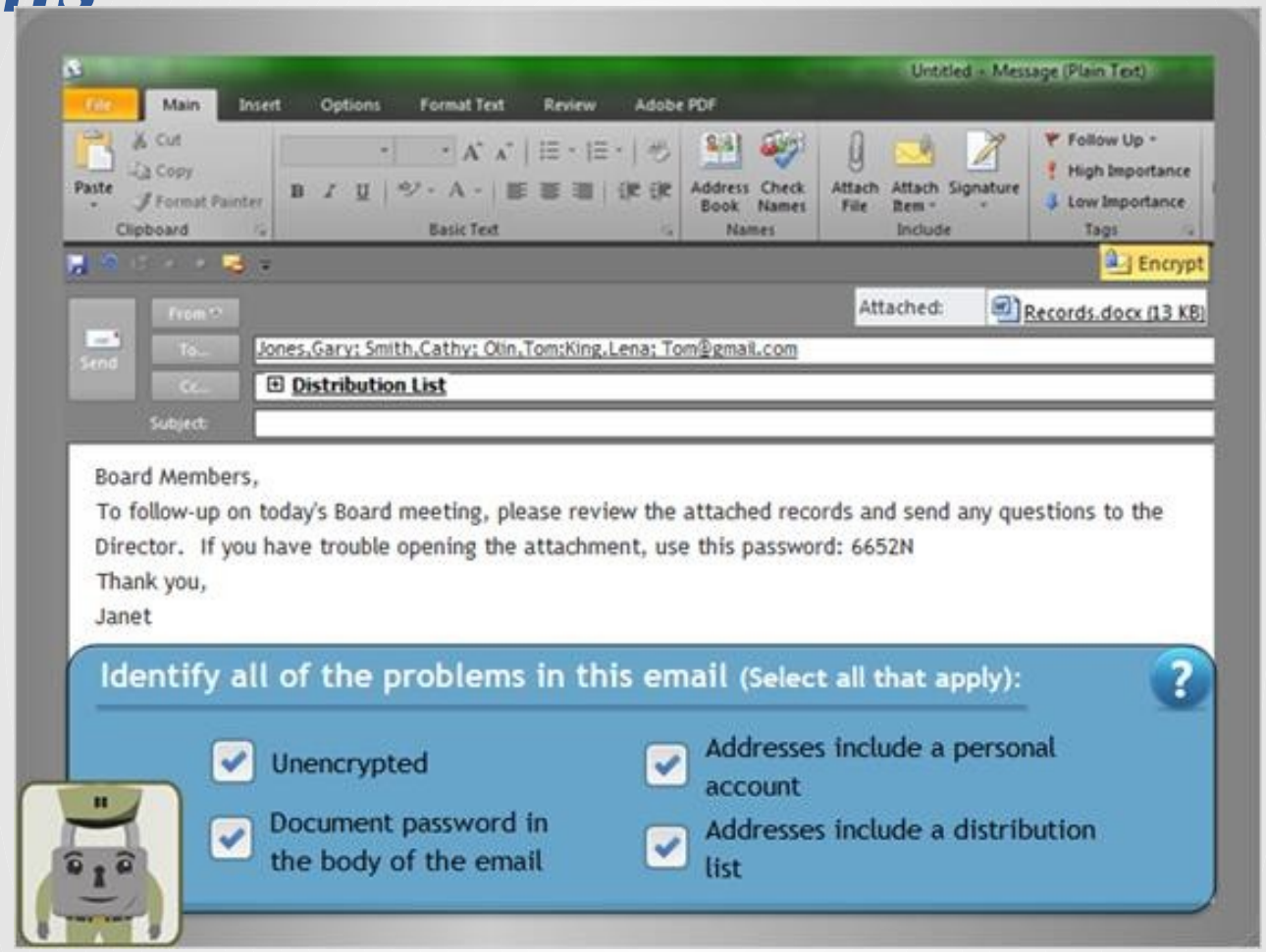
Scene 11
Office Cubicle: Dissemination

11.1 Email Communications

@4:00 FRI 22ND
TODO
CALL JIM!
heduled to review the concerns of the
ease see attached for the details and RSVP
can.
rs for your support and expertise.

Janet: *Oh, Private C, I didn't see you come in. I'm so glad you're here. I really need your help. Captain Carson asked me to email some of the records we discussed in today's board meeting. I've never emailed to the whole board before. Can you look over this email before I send it?*

11.2 Knowledge Check 1: Secure Emails

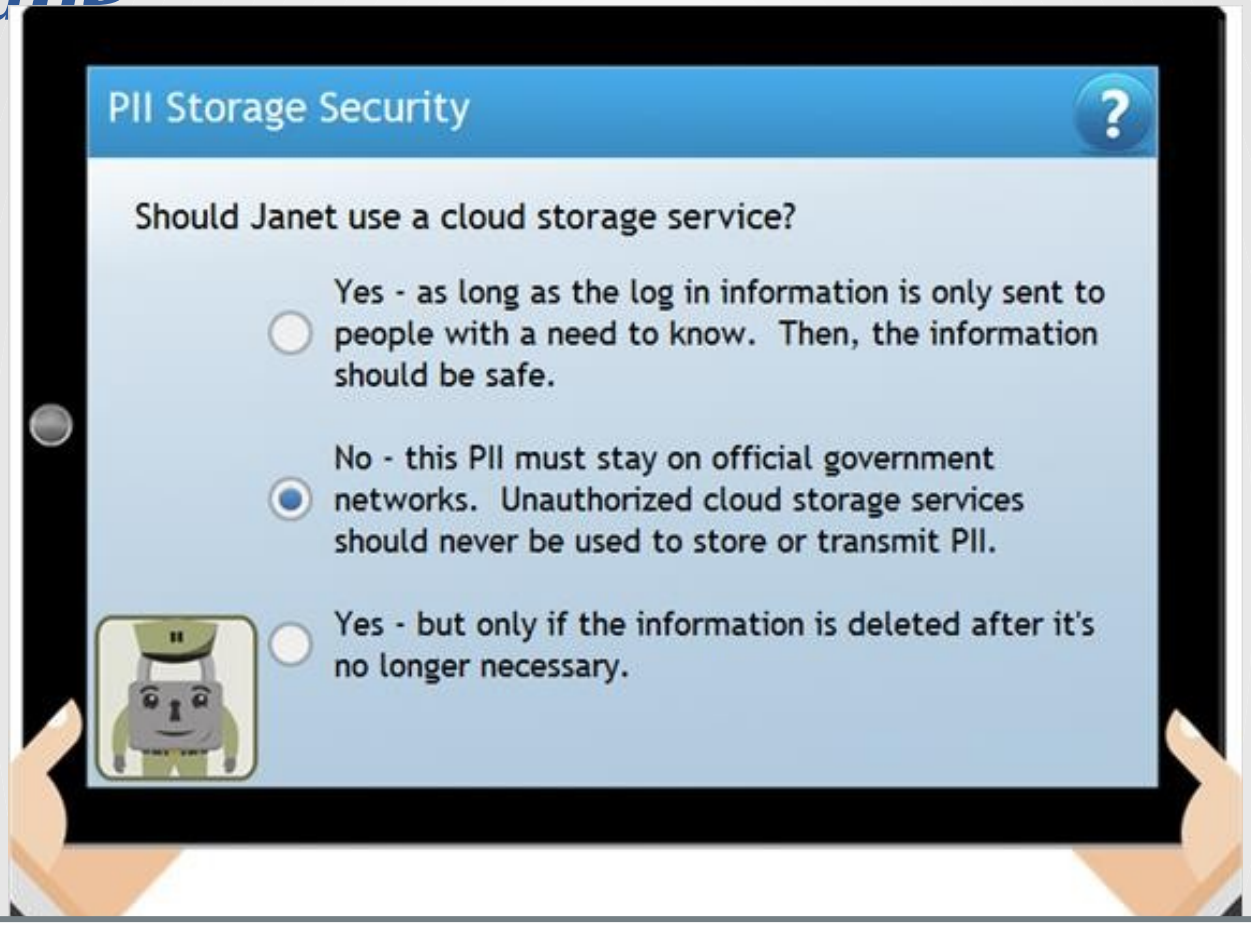


Captain Padlock: *TEMPCOM's computers show a high probability that this email could be the source of our breach. Look over it carefully, and fix any privacy concerns you can find.*

11.3 Cloud Storage

Janet: *Oh my goodness, I didn't even think about that, but you're right, I could have compromised that information. I'll fix it all before I send it... Hmm, I can't seem to get my email program to encrypt properly. What should I do? Oh, I suppose I'll upload it to my Cloud-U-Store account and just send everyone the log in information so that they can download it from there.*

11.4 Knowledge Check 2: Cloud Storage


PII Storage Security
?
Should Janet use a cloud storage service?
Yes - as long as the log in information is only sent to people with a need to know. Then, the information should be safe.
No - this PII must stay on official government networks. Unauthorized cloud storage services should never be used to store or transmit PII.
Yes - but only if the information is deleted after it's no longer necessary.

Correct Answer

No - this PII must stay on official government networks. Unauthorized cloud storage services should never be used to store or transmit PII.

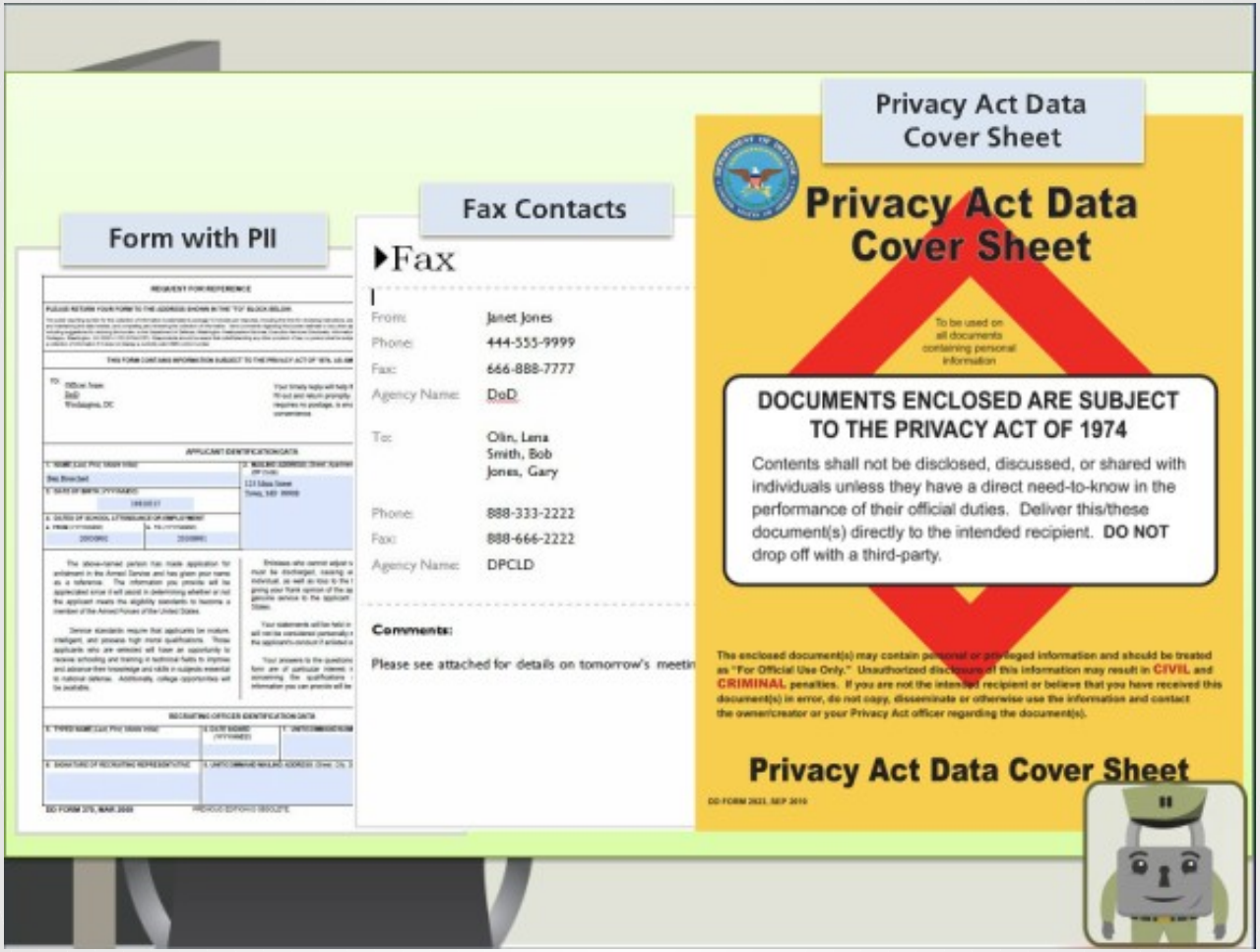
Captain Padlock: *When the Department collects or stores an individual's PII, we have an obligation to protect it and only release it to people with an authorized need to know, or pursuant to a published routine use of that information. Third party storage services don't have a need to know that information, and the security of anything loaded on those websites cannot be guaranteed. Even if the information is later deleted, cloud storage services can hold copies of that information on their*

11.5 Secure Faxes

Janet: *Gosh, you're right. I guess my only other option is to fax it to everyone. I have to run to a meeting, can you fax it out for me? Here's everyone's contact information.*

Captain Padlock: *It looks like she's taken care to ensure that all of the phone numbers are correct. Go ahead and send the fax.*

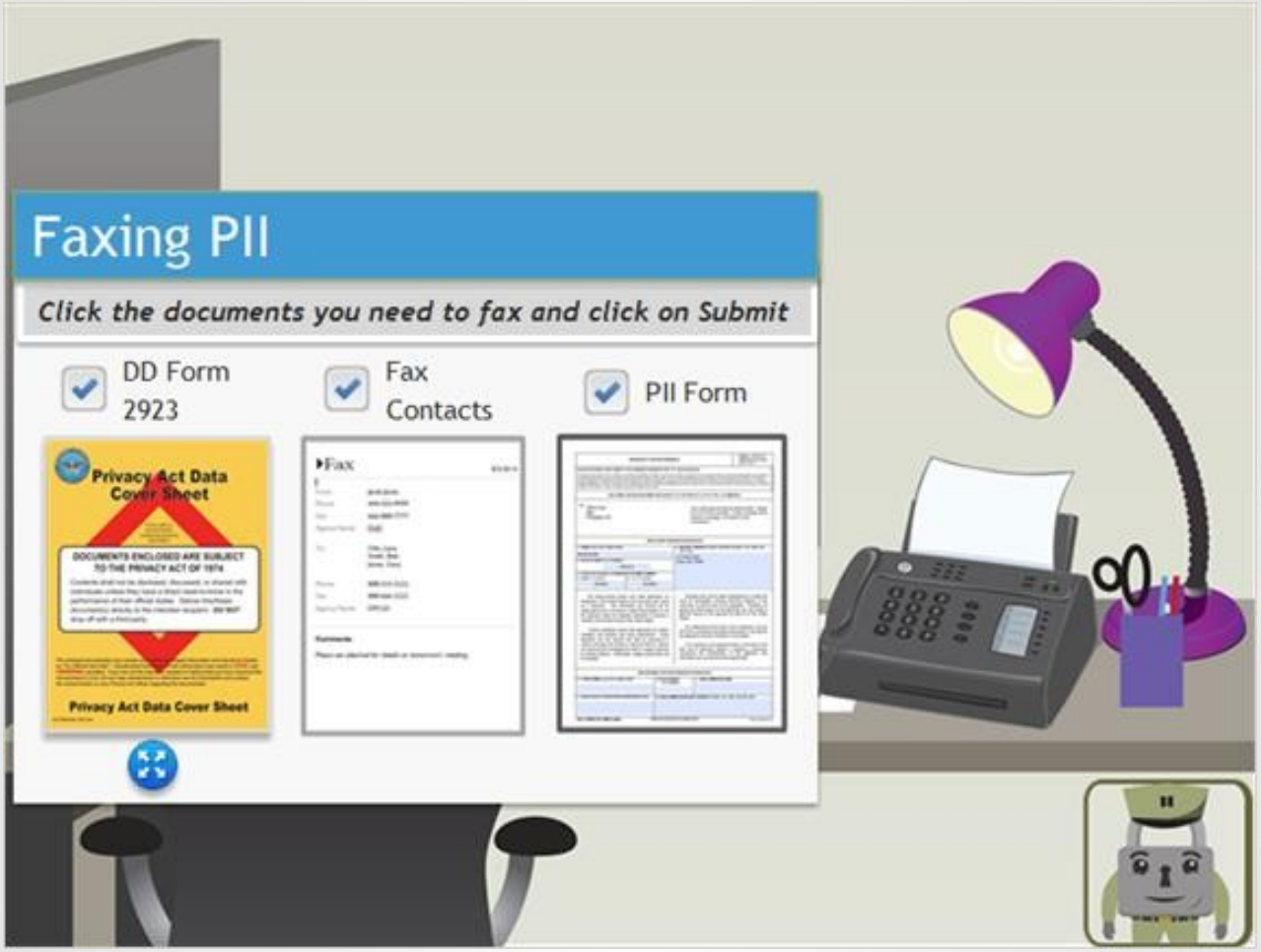
11.6 Fax Items


Form with PII
Fax Contacts
Fax
From: Janet Jones
Phone: 444-555-9999
Fax: 666-888-7777
Agency Name: DoD
To: Olin, Lena
Smith, Bob
Jones, Gary
Phone: 888-333-2222
Fax: 888-666-2222
Agency Name: DPCLD
Comments:
Please see attached for details on tomorrow's meetin
Privacy Act Data Cover Sheet
Privacy Act Data Cover Sheet
To be used on all documents containing personal information
DOCUMENTS ENCLOSED ARE SUBJECT TO THE PRIVACY ACT OF 1974
Contents shall not be disclosed, discussed, or shared with individuals unless they have a direct need-to-know in the performance of their official duties. Deliver this/these document(s) directly to the intended recipient. DO NOT drop off with a third-party.
The enclosed document(s) may contain personal or privileged information and should be treated as "For Official Use Only." Unauthorized disclosure of this information may result in CIVIL and CRIMINAL penalties. If you are not the intended recipient or believe that you have received this document(s) in error, do not copy, disseminate or otherwise use the information and contact the owner/creator or your Privacy Act officer regarding the document(s).
Privacy Act Data Cover Sheet

Scene Description

Documents and contact information required for sending a secure fax.

11.7 Knowledge Check: Faxing


Faxing PII
Click the documents you need to fax and click on Submit
DD Form 2923
Fax Contacts
PII Form
Privacy Act Data Cover Sheet
DOCUMENTS ENCLOSED ARE SUBJECT TO THE PRIVACY ACT OF 1974
Privacy Act Data Cover Sheet
Fax

Correct Answer
DD Form 2923, Fax Contacts and PII Form

Captain Padlock: *Good work! Whenever you fax PII, the cover sheet must include a Privacy Act warning statement. You will also want to include the Privacy Act Data Cover Sheet, DD Form 2923. The DD Form 2923 should also be used whenever a package containing PII is hand delivered or mailed.*

11.8 DoD Fax Form

Faxing PII
Click the documen
DD Form 2923
Privacy Act Data Cover Sheet
Privacy Act Data Cover Sheet
CLOSE
To be used on all documents containing personal information
DOCUMENTS ENCLOSED ARE SUBJECT TO THE PRIVACY ACT OF 1974
Contents shall not be disclosed, discussed, or shared with individuals unless they have a direct need-to-know in the performance of their official duties. Deliver this/these document(s) directly to the intended recipient. DO NOT drop off with a third-party.
The enclosed document(s) may contain personal or privileged information and should be treated as "For Official Use Only." Unauthorized disclosure of this information may result in CIVIL and CRIMINAL penalties. If you are not the intended recipient or believe that you have received this document(s) in error, do not copy, disseminate or otherwise use the information and contact the owner/creator or your Privacy Act officer regarding the document(s).
Privacy Act Data Cover Sheet
DD FORM 2923, SEP 2010

Scene Description

A zoomed in view of the DD Form 2923 – Privacy Act Data Cover Sheet.

11.9 Breach Averted

Captain Padlock: *Stand by....*

Scene 12
Fifth Time Travel: Case Solved

12.1 Final Time Travel: Breach Averted

Scene Description

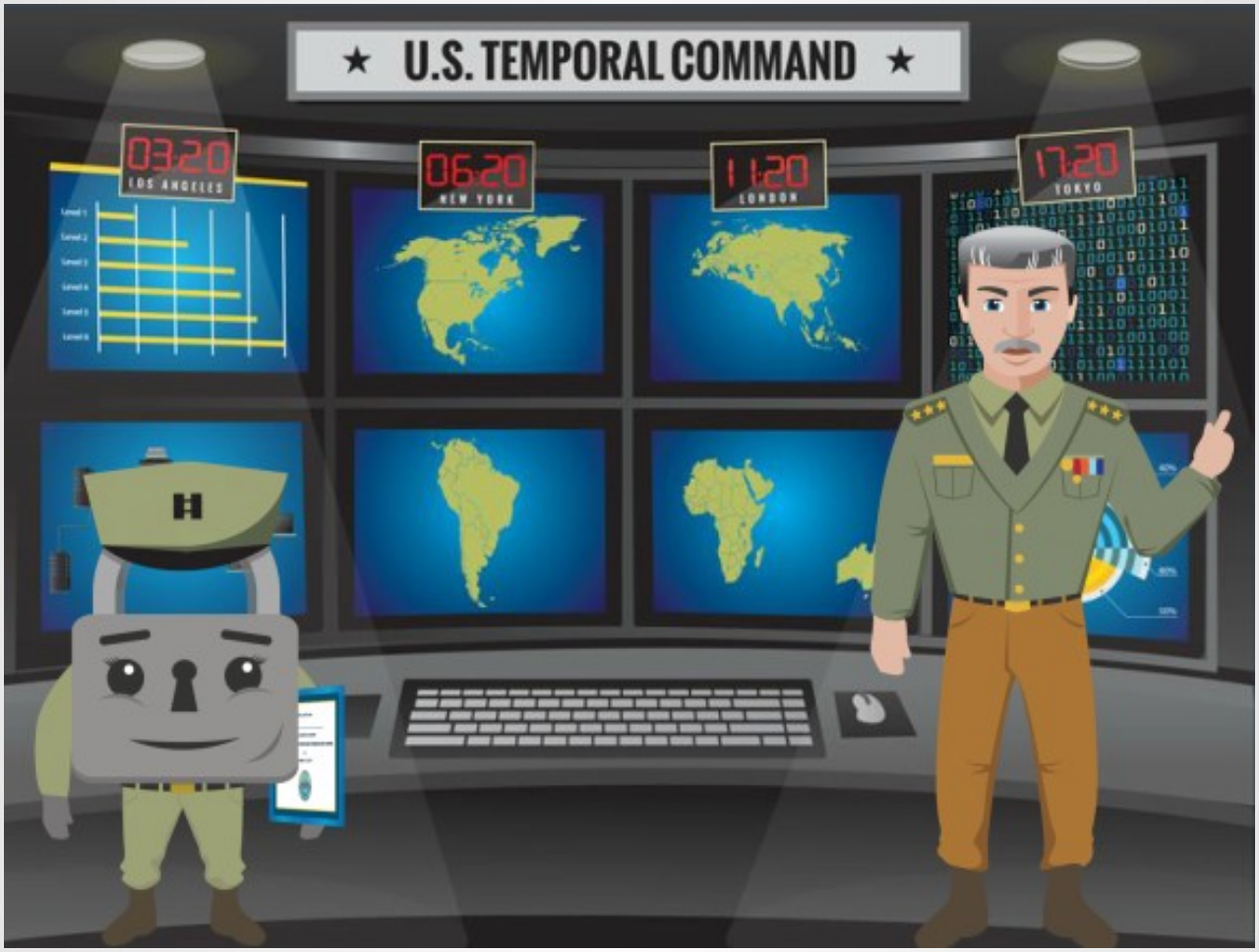
Final Time Travel screen with a simulation effect of graphics, sound and movement.

12.2: Remediation Complete

Captain Padlock: *We're still finishing up our latest calculations… yes… I believe… confirmed, the timeline has normalized and the breach has been averted! Excellent work Private C. Report back to TEMPCOM for your debriefing.*

Scene 13
Mission Complete

13.1 Mission Complete



General Relativity: *Oh Private C, I didn't see you come in. Excellent work out there. We've double checked our mission logs, and everything seems to be in tip-top shape. Ben Breached has never had his identity stolen thanks to you. And your work out there in the field may prevent even more people from falling victim to those criminals. I'd like to thank you for your work and present you with this certificate of our appreciation.*

13.2 Certificate of Completion

Scene Description

The course certificate is displayed in full screen to view with an option to print. Click the Next button to continue.

Scene 14
Review and Exit Course

14.1 Return to Training Center

Scene Description

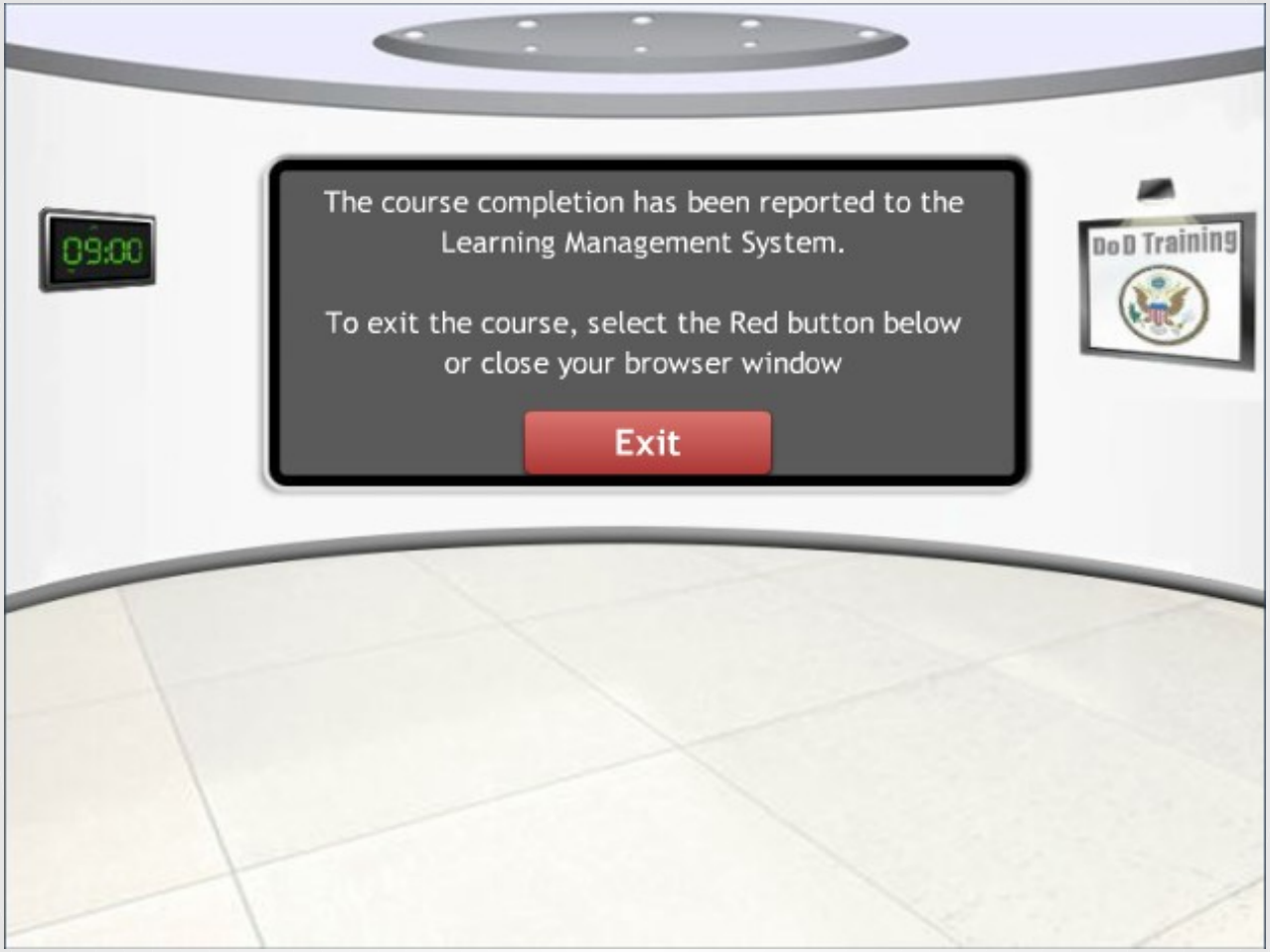
The Temp Command scene with Private C's tablet displaying an interactive button to "Return to Training Center".

14.2 Learning Outcomes

Scene Description

Congratulations! You have completed the Safeguarding PII course. For a recap of the Learning Outcomes, click the green button. To complete the course, click the blue button.

14.2 Exit Course


09:00
The course completion has been reported to the Learning Management System.
To exit the course, select the Red button below or close your browser window
Exit
DoD Training

Scene Description

The course completion has been reported to the Learning Management System. To exit the course, select the Red button below or close your browser window.